NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PERFORMANCE MANAGEMENT AN ANALYSIS OF AN IPv6 SENSOR ON THE MOVE USING COMMERCIAL NETWORK MANAGEMENT SOFTWARE

by

Adrian S. Adame
Bruce Kong

June 2008

Thesis Advisor:	Alex Bordetsky
Second Reader:	Michael Clement

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June 2008	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE **Performance Management an Analysis of an IPv6 Sensor on the Move Using Commercial Network Management Software**	5. FUNDING NUMBERS
6. AUTHOR(S) Adrian Adame & Bruce Kong	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Internet Protocol version 4 (IPv4) has been the internet standard since specified nearly 27 years ago. Although IPv4 has served us well the ever-growing demand for additional IP addresses has lead to the introduction of a new IP version, IPv6. Supported by Internet Engineering Task Force (IETF) for more than 10 years, IPv6 is recognized as a critical enabling technology throughout the federal government. IPv6 is also necessary in order to support the continuing growth of global communication requirements within Special Operations Forces (SOF); and ensure that the global Internet can continue to support a growing international user base and the increasing number of IP-enabled devices.

Although numerous network management studies have been conducted few have concentrated on tactical or edge network management. Furthermore, few studies identify potential management tools supporting usability within the GIG. In coordinated effort with our primary sponsor, U.S. Special Operations Command (SOCOM), the Naval Postgraduate School (NPS) has developed the Tactical Network Topology (TNT) field experimentation program aimed at providing solutions for today's battle space. TNT facilitates the examination of network management through the functional area of performance management and will serve to identify the tool that best supports network management of IPv6 tactical networks with IPv4 components.

14. SUBJECT TERMS IP, Global Information Grid, Network-Centric Warfare, Tactical Network, Network Management, Internet Protocol Version 6	15. NUMBER OF PAGES 93
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

PERFORMANCE MANAGEMENT ANALYSIS OF IPv6 SENSOR ON THE MOVE USING COMMERCIAL NETWORK MANAGEMENT SOFTWARE

Adrian S. Adame
Captain, United States Marine Corps
B.A., University of New Mexico, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
SEPTEMBER 2008

Bruce Kong
Lieutenant Commander, United States Navy
B.A., University of Hawaii, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
JUNE 2008

Authors: Adrian S. Adame

Bruce Kong

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Michael Clement
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Internet Protocol version 4 (IPv4) has been the internet standard since specified nearly 27 years ago. Although IPv4 has served us well the ever-growing demand for additional IP addresses has lead to the introduction of a new IP version, IPv6. Supported by Internet Engineering Task Force (IETF) for more than 10 years, IPv6 is recognized as a critical enabling technology throughout the federal government. IPv6 is also necessary in order to support the continuing growth of global communication requirements within Special Operations Forces (SOF); and ensure that the global Internet can continue to support a growing international user base and the increasing number of IP-enabled devices.

Although numerous network management studies have been conducted few have concentrated on tactical or edge network management. Furthermore, few studies identify potential management tools supporting usability within the GIG. In coordinated effort with our primary sponsor, U.S. Special Operations Command (SOCOM), the Naval Postgraduate School (NPS) has developed the Tactical Network Topology (TNT) field experimentation program aimed at providing solutions for today’s battle space. TNT facilitates the examination of network management through the functional area of performance management and will serve to identify the tool that best supports network management of IPv6 tactical networks with IPv4 components.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

ARP	Address Resolution Protocol
ASD NII	Assistant Secretary of Defense for Networks and Information Integration
CENETIX	Center for Network Innovation and Experimentation
CIO	Chief Information Officer
CMIP	Common Management Information Protocol
COTS	Commercial off-the-shelf
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DOD	Department of Defense
EA	Enterprise Architecture
FCAPS	Fault, Configuration, Accounting, Performance and Security
FY	Fiscal Year
GIG	Global Information Grid
GOTS	Government off-the-shelf
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Standards Organization
ITU-T	International Telecommunications Union
JITC	Joint Interoperability Testing Command
LLNL	Lawrence Livermore National Laboratory
LRV	Light Reconnaissance Vehicle
MIB	Management Information Bases
NAT	Network Address Translators
NCOW	Network Centric Operations and Warfare

NM	Network Management
NOC	Network Operations Center
NPS	Naval Postgraduate School
OFDM	Orthogonal Frequency Division Multiplexing
OMB	Office of Management and Budget
OS	Operating System
OSI	Open Systems Interconnect
SATNET	Satellite Packet Network
SIE	SOF Information Enterprise
SNMP	Simple Network Management Protocol
SOCOM	Special Operation Command
SOF	Special Operational Forces
STAN	Surveillance, Targeting, and Acquisition Network
TCP	Transmission Control Protocol
TNAT	Traditional Network Address Translators
TNT	Tactical Network Topology
UAV	Unmanned Aerial Vehicle

ACKNOWLEDGMENTS

Adrian Adame – First and foremost, I want to extend my deepest gratitude to my wife and children (Rose, Adrian Jr, Victoria, and Eva) for their never-ending support throughout my academic endeavor at the Naval Postgraduate School. I am forever grateful, to them. Thank you for you patience and understanding.

Bruce Kong – To my wife, Gemma, thank you for blessing me with unconditional love and unending support throughout my career. Your job is unquestionably the hardest, yet you consistently persevere with a cheerful, gracious and caring heart. Your unwavering commitment to our kids and me has proven to be the cornerstone of my every accomplishment. I am indeed extremely lucky to have you in my life.

We would also like to thank Doctor Alex Bordetsky and Michael Clement for providing the creative insight and forward thinking that resulted in this project. Their inspiration resulted in our ability to explore previously uncharted regions. The combination of your genuine enthusiasm and sharp intellect are unmatched at this institution. Additional thanks to Albert “Buddy” Barreto for allowing us access to equipment on very short notice, without your resourcefulness we could not have completed our research. To our classmates and academic peers, thank you for lending us your expertise and shoulder’s to lean on when things got hard.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

In August of 2005, the Office of Management Budget issued Memorandum 05-22, “Transition Planning for Internet Protocol Version 6 (IPv6)”, establishing the goal of enabling all Federal government agency network backbones to support the next generation of the Internet Protocol by June 30, 2008 (OMB, 2005). In response to Memorandum 05-22, the Department of Defense (DoD) mandated the creation of the DoD IPv6 Master Plan in order to meet IPv6 requirements by end of fiscal year (FY) 2008 (CIO, 2005). In accordance to the DoD IPv6 Transition Plan of February 2006, all Global Information Grid (GIG) assets being developed, acquired, or implemented are to be IPv6 capable while maintaining interoperability with IPv4 systems (CIO, 2006). The Defense Information System Agency (DISA) is responsible for the acquisition and management of all DoD IPv6 address schemes; to include the establishment of address and naming conventions.

Given the transition plans currently in place it is expected the deployment of IPv6 will begin at the core infrastructure (IPv6, 2006) of the GIG, and move outward toward tactical networks. Currently, tactical networks are built on the IPv4 stack; consequently, many of the devices currently in use cannot be upgraded to adequately support IPv6 datagram.

Although many network management studies have been conducted, there is little to no effort concentrated on tactical or edge network management in order to identify potential management tools to support usability within the

GIG. Tactical Network Management will be the focus of this thesis in the context of the Tactical Network Topology (TNT) field experiment program and United States Special Operation Command (USSOCOM) requirements. The Open Systems Interconnect (OSI) Network Management Model, commonly referred to as the FCAPS model, will be used to establish metrics to be tested on the TNT experimentation platform offered through the Naval Post Graduate School (NPS). This thesis was facilitated by the coordinated efforts of NPS faculty, students, and USSOCOM personnel.

A. BACKGROUND

The Internet is a worldwide network of networks comprised of servers, routers, and backbone networks. Network addresses are used to help send information from one computer to another over the Internet by routing the information to its final destination. The protocol that enables the administration of these addresses is the Internet Protocol (IP). The current version of IP is version 4. With the continuing growth of the global Internet, the Internet Engineering Task Force (IETF) recognized that IPv4 would soon be unable to support unique global communications. Under IPv4, the maximum number of unique 32-bit addresses is 2^{32} or 4,294,967,295 addresses. Although this seems like a very large number, it is much too small for tomorrow's Internet.

Ever-growing demand for additional IP addresses has lead to the introduction of a new IP version, IPv6, with over 2^{128} (3.4×10^{38}) IP addresses (Morton, 1997). IPv6 has been supported by IETF for more than 10 years, and is recognized as a critical enabling technology throughout the

federal government. IPv6 is also necessary in order to support the continuing growth of global communication requirements within Special Operations Forces (SOF); and ensure that the global Internet can continue to support a growing international user base and the increasing number of IP-enabled devices.

Network management of IPv4 has been a central issue in building every professional network. In the past, the monitoring, control and configuration of IPv4 network infrastructures was accomplished with independent software and often human intervention. The exponential growth of public IP networks and increased complexity of network technology made that approach to network management unfeasible. While the current solution(s) to monitoring, controlling and configuring network topologies under IPv4 are acceptable, achieving the same level of control becomes difficult when IPv6 is deployed. The huge address space which prevents the use of any iterative method is, among others, a feature that makes the problem challenging.

In order to ensure consistent IPv6 management of information technology and support throughout the federal government, OMB Memorandum 05-22 was issued in August of 2005 with the goal of enabling all Federal government agency network backbones of supporting the next generation Internet Protocol version 6 by June 30, 2008 (OMB, 2005). The memorandum directs all agencies, 24 in total, to complete two inventories of IP devices and technology, complete an IPv6 impact analysis, and develop an IPv6 transition plan. The CIO Council Architecture and Infrastructure Committee was tasked to develop additional

guidance and to address any major unforeseen elements in implementing IPv6 (OMB, 2005). As part of their enterprise architecture (EA) assessment, agencies were to provide a progress report on the inventory and impact analysis by February 28, 2008 (OMB, 2007). Results of the FY07 Federal Enterprise Architecture Assessment indicate that 19 of 24 reporting agencies are on track to meet IPv6 compliance as set forth in IPv6 Transition Plans (FEA, 2007).

B. PURPOSE OF STUDY

The purpose of this research is to identify tools that best support network management of IPv6 tactical networks with IPv4 components. This thesis will conduct an analysis of tools currently used by DoD and the status of future tools being designed by industry to determine areas of concern, which can potentially leave a hybrid or IPv6 only network vulnerable to malicious attacks.

C. THESIS QUESTIONS

The primary research question is: How can we manage tactical network IPv6 performance? The subsidiary questions are as follows:

- What challenges does SOCOM face in end to end IPv6 integration?
- How will SOCOM extend IPv6 to mobile sensors and nodes?
- How will mobile network design and equipment compatibility be affected?
- What are perspective network management architectures?

- What IPv6 management challenges are highlighted during TNT experiments in support of SOCOM research?

D. SCOPE AND LIMITATIONS

The scope of this thesis will encompass the analysis of network management tools currently used by DoD in order to evaluate and identify the best tool for management of IPv4 and IPv6 hybrid networks. The study will explore DoD and SOCOM transition requirements to establish the need for hybrid networks and subsequent management tools. The study will be conducted within the limits of the Center for Network Innovation and Experimentation (CENETIX) lab aboard NPS, and TNT experimentation aboard Camp Roberts.

E. ORGANIZATION OF STUDY

This thesis is organized as follows:

Chapter II will provide an overview comparison of IPv4 to IPv6 and highlight DoD and SOCOM transition requirements. Chapter III identifies possible metrics that maybe used to measure the performance of network management tools. Chapter IV presents the products, devices experimentation used in the evaluation of Network Management tools to determine each tools ability to manage network performance as well as some of the challenges. Finally, Chapter V provides conclusions and recommendations for management of tactical networks; and suggestions for future work on the analysis and evaluation of the proposed solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTERNET PROTOCOLS COMPARED

A. INTRODUCTION

IPv4 has been the internet standard since it was specified nearly 27 years ago. This chapter summarizes the design of both the current protocol, IPv4, and the future Internet Protocol, IPv6. The protocol design summaries are followed by a discussion of Mobile IPv6, a protocol allowing mobile nodes to move from one network to another without losing connectivity. The Mobile IPv6 discussion is followed by the comparison of IPv4 and IPv6. The final section introduces the need for the transition to IPv6 within the DoD.

1. Header Structure

The simplified header structure of IPv6 facilitates greater flexibility and functionality; primarily, a result of the new IPv6 fixed header size. In contrast, IPv4 header size can vary from 20 to 60 bytes (Loshin, 2004), depending on whether or not and what type of options are used. The larger the header size, the longer it will take to route information. Depending on whether or not options are used an IPv4 header can contain 12 to 14 different fields required to complete a packet header. The 14 fields in IPv4 are streamlined to only 8 in IPv6 and come as the result of elimination, renaming, or reorganization of the various data fields (GAO, 2005).

a. IPv4 Options

The options field varies in length dependent on the number of options included and the varied non-static size of most options (O'Neal, 2003). The following is a short list and brief description of options as outlined in RFC 791.

- Security – Security, compartmentation, restrictions handling, Transmission Control Code information.
- Loose Source Routing – Specifies a route that is indirect and allows the use of any route and may include any number of intermediate gateways to reach the next address in the route.
- Strict Source Routing – Specifies a route that includes only the directly connected network as indicated in the next address to reach the next gateway or host as specified in the route.
- Record Route – Records the address of each node that processes the packet.
- Stream Identifier – Allows the 16-bit Atlantic Satellite Packet Network (SATNET) stream identifier to be carried through networks not supporting the stream concept.
- Internet Timestamp – Inserted by every node that processes the packet.

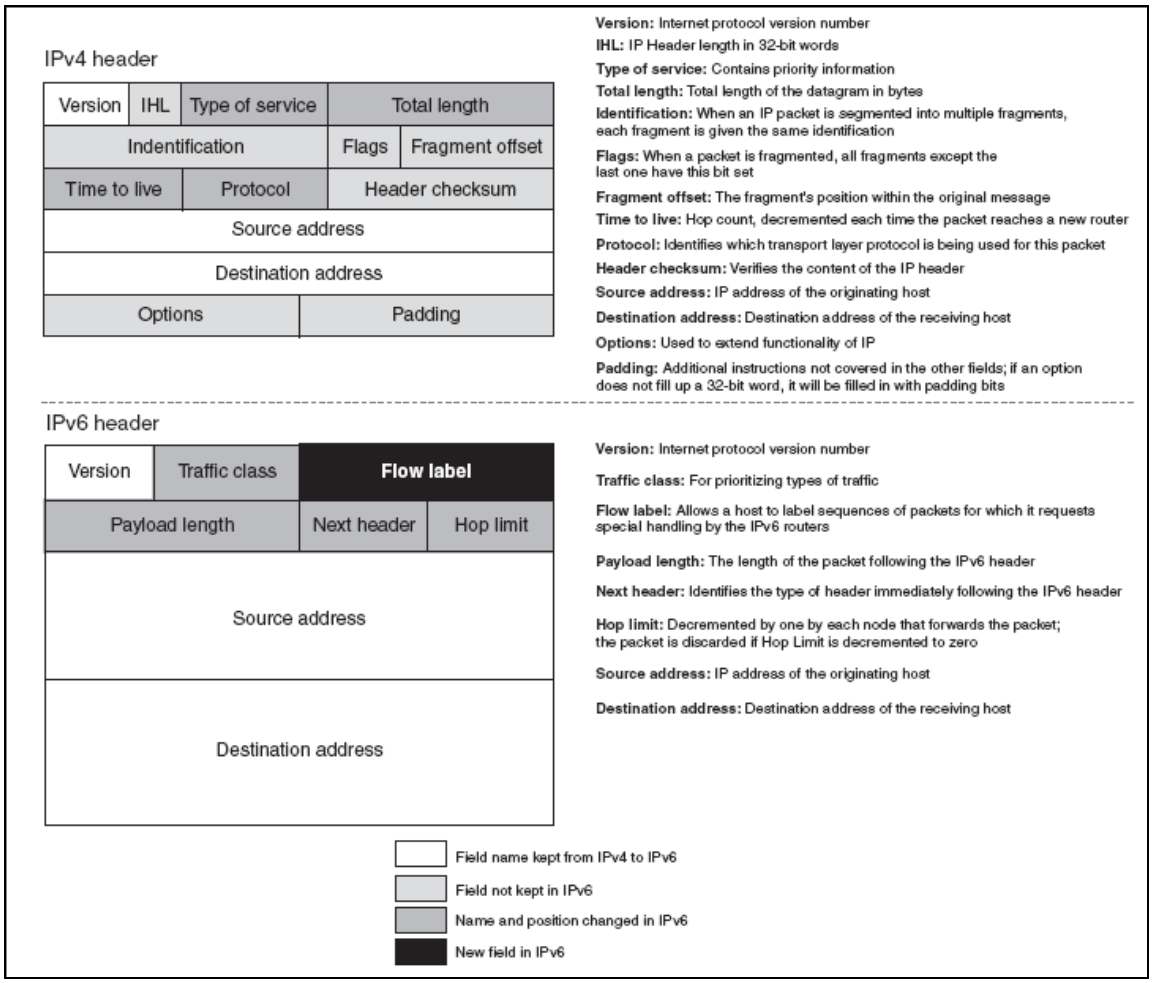


Figure 1. IPv4 and IPv6 Headers Compared (GAO, 2005)

2. Security

Originally intended to serve as a simple internetworking protocol, IPv4 was not designed to offer security features (Loshin, 2004). Although not a problem given IPv4 was primarily used in research and academic environments it has increasingly become a problem as business and consumer networking environments become more prevalent. Consequently, the possibility for devastating damage to individuals and organizations from attacks is more likely. To protect against potential damage, Internet

Protocol Security (IPSEC) was introduced as an enhancement to IPv4 (Dean, 2006). IPv6 is considered a “more secure” protocol as a result of better integrated authentication and encryption capabilities consisting of two header extensions capable of working together or separately to improve authentication and confidentiality (GAO, 2005). The primary difference between how IPv4 and IPv6 use IPSEC and level of security offered by each protocol comes as a result of how each implements IPSEC. In IPv4, the use of IPSEC is optional, yet IPSEC support is mandated, as part of the IPv6 protocol stack (Doan, 2006). Although IPSEC support is mandated for IPv6, implementation is still optional and likely not to be used given the complexity of configuring and administering, specifically as it pertains to large networks. In fact, many current IPv6 implementations do not include IPSEC (IPv6, 2006). As a result, IPv6 continues to be vulnerable to application layer attacks, sniffing, rogue devices, Man-in-the-Middle Attacks, and flooding (Cisco, 2006).

3. Address Space

Theoretically, the IPv4 address space provides a maximum of 2^{32} addresses, which translates to approximately 4.29 billion 32 bit addresses (Hagen, 2006). In contrast, IPv6 is a 128 bit address scheme capable of supporting approximately 3.4×10^{38} addresses (GAO, 2005). The significant increase in address space essentially means that an IP address can be assigned to almost any electronic device.

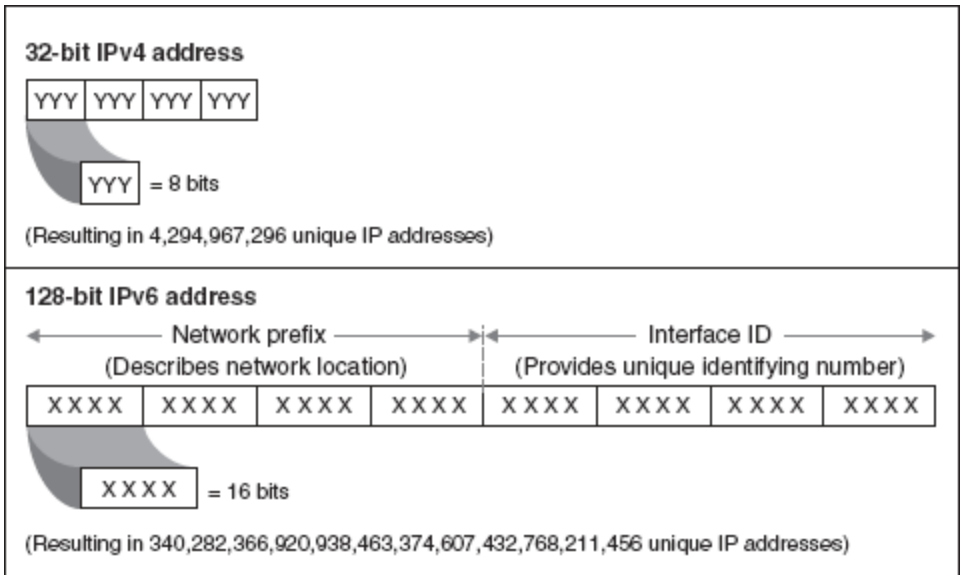


Figure 2. IPv4 and IPv6 address space compared (GAO, 2005)

IPv4 is divided into 5 distinct and hierarchical classes intended to serve the needs of organizations varying in size. However, only three A, B, and C are commonly used and represented in Figure 3.

Network Class	Beginning Octet	Number of Networks	Maximum Addressable Hosts per Network
A	1–126	126	16,777,214
B	128–191	>16,000	65,534
C	192–223	>2,000,000	254

Figure 3. Commonly Used TCP/IP Classes (Dean, 2006)

Class D address space is reserved for multicasting and therefore unable to define a network address; however for class distinction beginning octet values assigned to class D addresses range between the values 224 – 239. Class E

address space begins with an octet value between 240 and 254, and is reserved for the IETF to use for research and other non-routable purposes. Neither Class D or E addresses should be assigned to networked devices.

Given the large number of addresses available to IPv4 users, one might assume that the allotted address space as outlined above would be sufficient to support the every need of the world's internet users; unfortunately, this is not the case. Despite a larger number of internet users in Europe and Asia the United States received the larger address allocation (Kay, 2006). As a result, countries in Europe and Asia have been forced to seek alternative methods to route information and link hardware, ultimately leading to their transition to IPv6. To ease the poor management and availability of IPv4 addresses Network Address Translators (NAT) were introduced.

4. Network Address Translation

First specified in RFC 1631 as a short term solution, and later updated by RFC 3022 in 2001; NAT allows the use of private address space within a local network for internal communication and at least one global address for external communication (Forouzan, 2003). Conceptually, requirements to successfully implement NAT are limited to a single connection to the Internet via a router capable of running NAT software; however, for a NAT environment to properly function all border network devices require NAT functionality (Baumgartner, 2004). That is to say, when a node within a private network using a private IP address wants to send a packet to a destination not within the same private network, a NAT enabled device is required to

translate. The NAT enabled device acts as a go-between using the private IP address as the source and the remote node's IP address as the destination. All data-grams, in or outbound are routed through a NAT device to ensure that outbound data-grams are rewritten using the NAT device's global address as the source; leading the destination node to believe that the packet has originated from the NAT device. When the destination node responds the data-gram is sent to the NAT device where it must be rewritten and addressed to the appropriate private address using routing and look-up tables. The description outlined above is the basic premise of NAT, also known as Traditional NAT (TNAT), although multiple variations of NAT exist we focus on TNAT to establish the basic framework of IPv4 and the need to transition to IPv6. Despite NAT's effectiveness in decreasing the strain on the IP address pool NAT is not free of problems and is known to create problems with some protocols and applications used in a NAT environment.

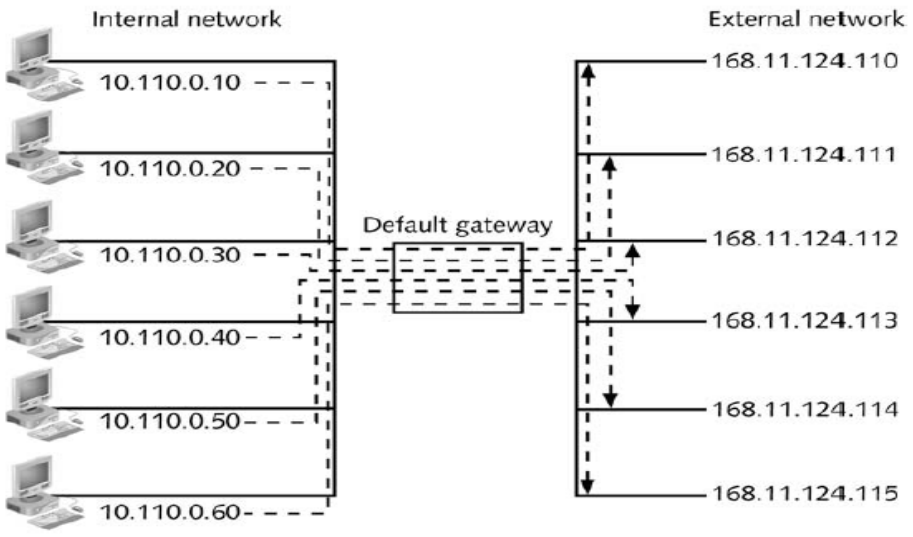


Figure 4. NAT through an Internet gateway (From: Dean, 2006)

As IPv4 reaches the end of its useful lifespan, following the internet's growth by approximately 10 million times its original size since 1981 (Loshin, 2003), IPv6 was introduced to mitigate the foreseeable shortcomings of IPv4. Specifically addressed by IPv6 is the demand for more mobility and transparency as the use of notebook computers, wireless networks, and portable devices is expanding (Hagen, 2006).

5. Mobility

Mobility is most often coupled with wireless technologies that facilitate rapid movement over long distances (Comer, 2000). However, Speed is typically not the problem when discussing mobility; instead the issue is the movement of a host from one network to another, specifically as it pertains to IPv4. By design, IPv4 is optimal for stationary networks where a node's IP address serves to identify a unique point of attachment to the internet (Perkins, 2002). Consequently, in order for host A to receive datagrams from host B, it [host A] has to be on the network to which its IP address is assigned. Connecting host A to a new network invalidates its current IP address and requires that either:

- The host change its address.
- Routers propagate a host-specific route across the entire internet.

In either case, the work involved is often not worth the effort of making the change since changing the address breaks all transport layer connections; and host-specific

routing is not scalable (Comer, 2000). Mobile IPv4, as specified in RFC 3344, allows for movement between Ethernet segments as well as from an Ethernet segment to a wireless LAN. However, the mobile devices IP address cannot change. As a result, mobility utilizing IPv4 is limited to the boundaries of a host's own point of attachment.

Mobile IPv6 takes lessons learned from the development of Mobile IPv4 and integrates them with improvements, only available through IPv6, (Johnson, 2004) to achieve the capability to move from one network to another without losing connectivity. Mobile IPv6 continues to support current methodology with the implementation of Stateful Autoconfiguration, which equates to DHCP. That is to say, hosts obtain interface addresses and/or configuration information and parameters from a server (Thomson, 1998). IPv6 improves upon Dynamic Host Configuration Protocol (DHCP) with the implementation of stateless autoconfiguration. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers (Thomson, 1998). IPv6 also brings added features such as optimized routing and traffic flow to mobile platforms. The advantage is that the shortest available path can be used and packets do not need to route through the home agent. Additionally, IPv6 brings added security and improved interoperability to mobile environments, however; IPSEC must be configured to secure data flow between the home agent and a mobile device (Dean, 2006).

The loss of connectivity during the "handover" from one network to another is undesirable and most often the

case under IPv4 architectures using NAT technologies. The mobility that is built into IPv6 is able to set data routing protocols to any terminal within range without interrupting the connection in progress. This is accomplished in part by the “neighboring node interaction” and the stateless auto-configuration inherent in IPv6.

> The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manage the interaction of neighboring nodes on the same link. Neighbor Discovery replaces the broadcast-based Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages (Microsoft, 2004).

Thus, IPv6 provides significant advantages over IPv4 in the use of mobile technologies. Because many Internet users have recognized the myriad of applications for wireless communications, the implementation of IPv6 will be a key factor in the successful use of mobile technologies.

Despite the advertised improvements, IPv6 is not perfect and presents its own set of mobility challenges. For example, although a mobile node can automatically configure itself to establish a connection to a new link, Transport layer connections, such as Transmission Control Protocol (TCP), made using the mobile node’s previous address can no longer be used (The Cable Guy, 2004). The move invalidates the previous address resulting in the need to abandon existing TCP connections. Consequently, applications need to make new connections using a newly assigned address. In addition, depending on the application, the change in IPv6 address configuration can cause an application to stop working and will require the

user to stop and restart the affected application. To achieve true roaming support, an IPv6 node has to support both auto-reconfiguration and Transport layer connection survivability (The Cable Guy, 2004).

Additional problems arise when IP mobility and IP multicast are coupled to support IP multicast for mobile hosts (Romdhani, 2004). Figure 5 outlines Mobile multicast challenges.

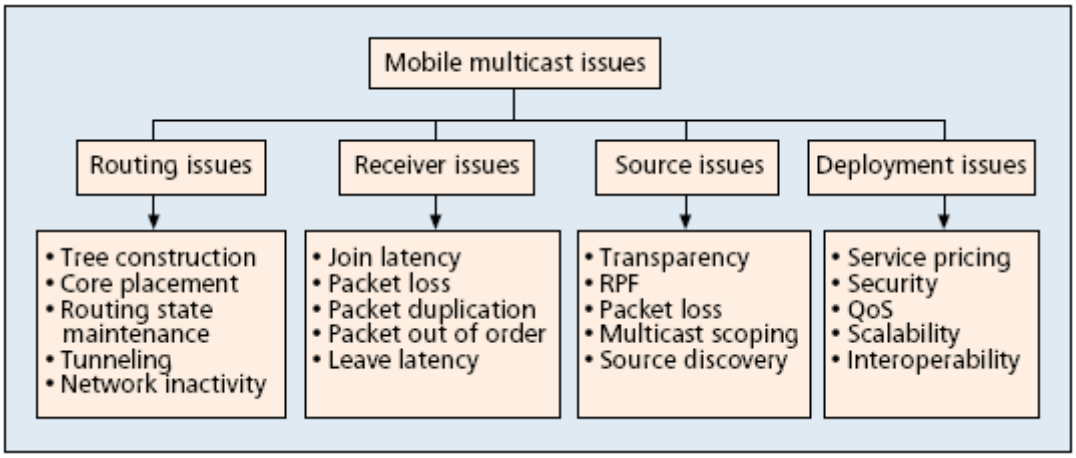


Figure 5. Mobile multicast Challenges (Romdhani et al, 2004)

Furthermore, mobile node handover is especially challenging. The complete handover of a mobile node is a six task process, some of which can be performed in parallel yet there is some requirement for sequential processing (Lundberg, 2003). Figure 6 illustrates a handover in Mobile IPv6.

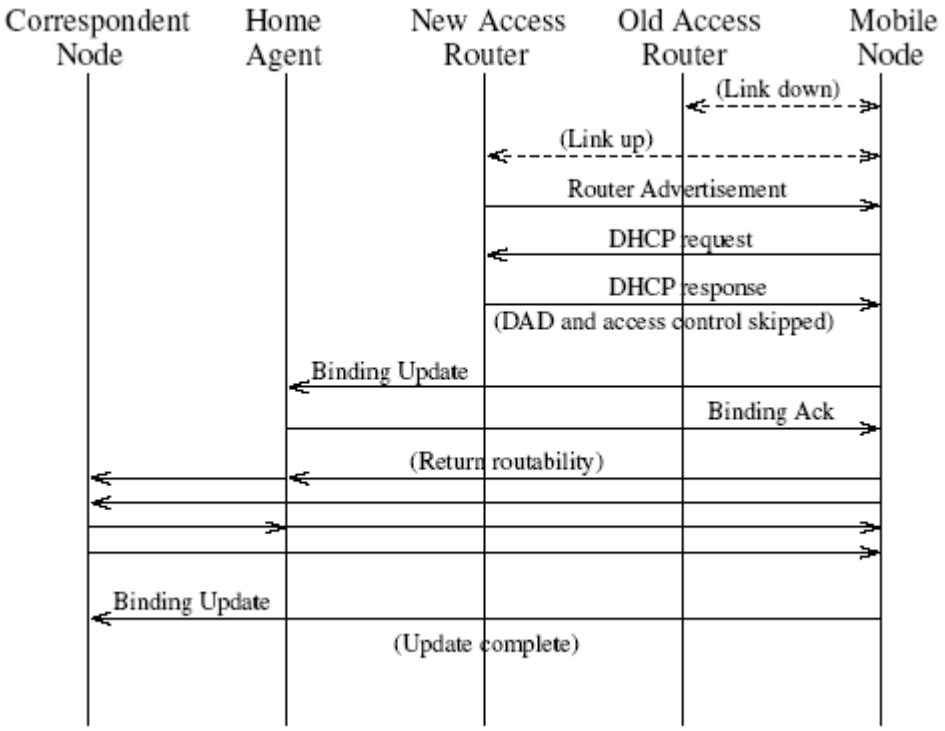


Figure 6. Mobile IPv6 Handover (Lundberg, 2003)

Steps 1-3 of the handover process are operations calling for open communications between the mobile node and devices within the access network. How long it takes for operations 2 and 3 to complete their process is dependent on the settings of equipment in the access network to which the mobile node is moving. Although some delays can be expected during the completion of operations 2 and 3 the latency experienced is concentrated in steps 4-6 due to high propagation delays while communicating with distant nodes. To initiate the handover procedure the mobile node will disconnect from the current access point and break established communications. The mobile node can only re-establish communications when the handover procedure has

completed all of its required tasks. As a consequence, all packets sent during the handover procedure are lost.

These challenges pose detrimental shortfalls that place undue burden on network administrators and tactical operators resulting in inefficient and unreliable communications. Nonetheless, these concerns are the subject of multiple studies for which solutions have been identified and published.

6. IPv6 Advertised Features and Benefits

With the demands placed on IPv4, specifically in the Network Centric environments within the DoD, the DoD has become a driving force behind the need to transition to IPv6. The need for real time information and Network Centric capabilities throughout the DoD are facilitated by the capabilities inherent within IPv6. The benefits of IPv6 are extensive; it is not simply a patch designed to further extend the life of the current protocol. Instead it is a redesign based on the fundamental core of IPv4 that keeps in mind the exponential growth potential of our networking requirements and desires. The Table 1 specifies the significant differences between the two protocols.

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPSec support is optional.	IPSec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).

Table 1. Comparison of IPv4 and IPv6 (From: GAO, 2005)

B. TRANSITION PLAN

1. DoD Transition Strategy

The DoD Transition Plan describes the overall strategy for the DoD's migration from IPv4 to IPv6 (ASD, 2006). It identifies roles and responsibilities and establishes the foundation for more in-depth analysis of possible commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) implementations of IPv6.

In a 9 June 2003 policy memorandum, the Assistant Secretary of Defense for Networks and Information Integration (ASD NII) established the goal of transitioning all DoD enterprise-wide networks from IPv4 to IPv6 (ASD, 2004). The memorandum set forth the goal of completing the transition by FY08. This transition plan envisions the evolution of each branch of services' operational networks into one network-centric entity, improving access to the warfighter knowledge base and institutional support systems, interoperability, mobility, security, reliability, scalability, and assured information integrity.

IPv6 is an enabling technology of network-centric operations and warfare which will include mobile platforms, networked sensors, unmanned systems, unmanned aerial vehicles, space systems, reach-back to logistics bases, facilities, people, and information (ASD, 2004). IPv4 is ubiquitous in all branch of services' networks today. It is used to address and move data throughout the services' tactical and institutional networks interfaced and interoperable with the GIG.

The IPv4 to IPv6 transition seems to be a significant challenge for all service branches. A large number of

hardware and software systems including applications will need to be upgraded or replaced. Major assessments will need to be made with regard to engineering, procurement, testing, and deployment. It is likely during the transition phase, new or modified IPv6 capable systems and applications will need to operate with the existing IPv4 systems and applications without degradation in performance, reduction in availability, or compromise of security (IPv6, 2008).

2. SOCOM Transition Strategy

The Special Operation Forces (SOF) Information Enterprise (SIE) Strategy Internet Protocol Version 6 document mandates SOCOM strategic action to transition the SIE from IPv4 to IPv6. The transition to IPv6 relies on centralized planning, testing, training, information assurance, and stable IPv6 standards. SOCOM's objective is to be able to transmit IPv6 traffic from Internet and external peers, through the network backbone, to the LAN, and to other LAN networks.

SOCOM's requirement is to ensure its infrastructure will be IPv6 enabled by FY08 for the unclassified network and FY10 for the classified network; per Defense Information Systems Agency's (DISA) IPv6 schedule (DISA, 2006). Transition of the classified network is delayed due to the unavailability of IPv6 enabled encryption devices currently scheduled for to be available in FY10 (USSOCOM, No Date Given).

3. Current State of IPv6 Network Management Within DoD

The adaptation of IPv6 within the DoD has experienced some delays; primarily the result of commercial vendor's putting a higher priority on other requirements within the communications industry (Kaushik, No Date Given). The demand placed on commercial vendor's by the DoD is considered a small portion of the greater communications industry. Although the DoD's influence is not the prevailing factor, many domestic companies have begun incorporating IPv6 capabilities into their hardware and software products. The two largest manufacturers of Internet routers, Cisco and Juniper, are industry leaders and the first to include IPv6 capabilities in their equipment over the last several years. Cisco estimated that about one-third of desktop computers currently deployed in the United States are IPv6-capable (IPv6, 2006). Notwithstanding, given the disparate makeup of most DoD networks we are lacking open standardized interfaces between the involved equipment and management software (Heilbronner, 1997) allowing network administrators the ability to monitor, control, and configure IPv4 and IPv6 hybrid or IPv6 only network infrastructures.

Network management systems under IPv4 have been in operation for many years especially in their own proprietary world (Stevenson, 1995). With the implementation of protocols such as Simple Network Management Protocol (SMNP), Net Flow, and Common Management Information Protocol (CMIP), local area and wide area network components can be monitored and managed efficiently with the help of vendor software and human intervention.

However, with the exponential growth of IP networking and the increased complexity of managing IPv6 networks has made the platform-centric manager-agent paradigm approach to network management unfeasible (Goldszmidt, 1998).

In today's DoD networking environment, the implementation of IPv6 must follow the vision of Net-Centric Operations and Warfare (NCOW) based on the GIG's inter-networked sensors, radios, platforms, facilities, people, and data (DISA, 2006). Although there has been a great deal of research done in addressing the core network implementation, IPv4 and IPv6 co-existence requirements and even cost analysis, there has been little to no analysis performed on how to manage IPv6 network components within the GIG. Integration of existing systems with new technologies will be a significant challenge as the DoD moves toward enabling a network-centric force (Alberts, 2000). Furthermore, network management is made especially challenging since most tools available for IPv6 are mere replacements of tools developed and used for IPv4 (Cho et al, 2004).

C. MANAGEMENT OF NETWORK

1. Primary Network Management Functionality

Regardless of the management functionality, all network elements must be able to provide their intended primary service (e.g. routing IP packets). However, the service must be somehow initialized, configured, monitored and controlled, which are within the network management domain. The objective for network management has been coined into a requirement to provide more effective, user-

friendly, standardized and flexible way to implement the management functionality (Makela, 1999).

Network management can be broadly defined as the assessment, monitoring, and maintenance of all managed objects (Dean, 2006). These objects behave as an integrated conglomeration of functions that may be located on one machine, in different support organizations, or within many machines and databases spanning thousands of miles. Each of these functions must be directly driven by the mission requirement or business case.

The monitoring of the network is one of the most crucial tasks for network management, since it provides information on the network status. The collected data can be used to reveal and prevent abnormal and undesirable situations, as well as to configure network parameters. A method often used to collect data is SNMP. This protocol provides a simple and uniform way to query network devices (Boutaba, 2002). Through SNMP commands, network managers can request values from the Management Information Bases (MIBs) of the managed devices. In addition, SNMP allows managers to set values in the MIBs, thus affecting the behavior of the managed devices.

2. FCAPS Management Model

Given its heterogeneity and size, a large network cannot be built and managed with human effort alone. The help of automated tools is essential to successful network deployment and exploitation. The most common framework depicted in network management designs is centered on the “FCAPS” model. The idea of FCAPS stems directly from the International Telecommunications Union (ITU–T)

recommendations M.3010 and M.3400 which describe the five different types of information handled by management systems (Parker, 2005). Theoretically, portions of each of the FCAPS functional areas are performed at different layers within a given architecture.

In 1997, International Standards Organization (ISO) delivered the FCAPS framework called the Open Systems Interconnect (OSI) Network Management Model as the basis for most network management implementations (Parker, 2005). Under the umbrella of network management the OSI model further specifies five functional areas (Parker, 2005). These functional areas are, **F**ault Management, **C**onfiguration Management, **A**ccounting Management, **P**erformance Management, and **S**ecurity Management.

Following is a brief explanation of each concept (Cisco, 2001):

- Fault Management. Fault Management is to detect, log, notify users of, and automatically fix network problems to keep the network running effectively. Because faults can cause downtime or unacceptable network degradation, fault management is perhaps the most widely implemented of the ISO network management elements.
- Configuration Management. Configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

- Accounting Management. The accounting management is to measure network utilization parameters so that individual or group users on the network can be regulated appropriately. Such regulation minimizes network problems and maximizes the effectiveness of prioritization of network access across all users.
- Performance Management. Is to measure and make available various aspects of network performance so that inter-network performance can be maintained at an acceptable level.
- Security Management. Security Management is to control access to network resources according to local guidelines so that the network cannot be sabotaged and sensitive information cannot be accessed by those without appropriate authorization.

Today’s modern network management solutions must deal with all the components described above. The challenge is in balancing the network management components between centralized and distributed approaches, and to maintaining a clear view of the network status and the elements involved in network operations. Further complicating matters is the requirement to manage legacy IPv4, IPv4 and IPv6 hybrid, or IPv6 only networks while providing the same information we’ve become accustomed to.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SELECTION OF METRICS

A. IDENTIFYING NETWORK METRICS

A metric is a “meaningful measure of the extent or degree to which an entity possesses or exhibits a particular characteristic” (DACS, No Date Given). It is designed to objectively measure and provide the predictive behavior(s) of desired attributes of a system. Many attributes can contribute to a useful metric for which there are numerous definitions and purposes, but good performance metrics have several key characteristics in common.

The first characteristic of good metric is that it can be observed and monitored over time. Snapshots of a system simply provide information pertinent to past activity. In management of network performance, historical information is useful, but information that allows the network manager the ability to predict and adjust on the fly is much more valuable in network centric applications. Metrics that can be tracked and graphed allow one to see trends, which provide vital visual characterization of network performance. The resulting network depiction makes it easier to forecast network behavior and facilitates network configuration adjustments (i.e. node or senor locations) to maximize network performance. A good metric will consistently measure the same item, a function that is crucial to comparison and trend analysis. Changing what is included in the metric after the outset of data collection invalidates the entire measurement process. As an example, throughput measurements must use the same packet size in

order to properly analyze bandwidth behavior. It is important that once a metric is analyzed, something can be done to change the metric or change the system in a way that results in a changed value for that metric. For example, if latency is too high, there needs to be some action that can be taken to change the metric used to measure latency. Finally, a good metric can be benchmarked amongst similar systems for comparison. For example, the throughput of a wireless MESH can be further analyzed when compared to a wired network throughput (Davis, 2005).

B. ESTABLISHMENT OF PERFORMANCE METRICS

Valuable network management performance metrics are functional, timely, and consistent. A good network management metric provides a complete picture of a networks' quality; and further enables network analysis permitting accurate predictability of network behavior(s). For the purpose of this thesis, the following seven metrics, as applied to the network management tools, are integral to monitoring the performance of IPv6 nodes while evaluating the utility of tested network management applications.

- Utilization and error rates
- Consistent performance level
- Performance data collection
- Performance data analysis
- Problem reporting
- Performance data and statistics collection
- Maintaining and examining historical logs

Specifically, the seven metrics will be measured by means of how well the individual tools are able to perform the stated function. This measure will be achieved through

a cross sectional matrix to facilitate the rating of each tool on a High, Medium, Low scale. The scale is further defined below.

- High (3) – The tool has full functionality in the measured area and is very capable of providing the requested output.
- Medium (2) – The tool is able to provide a reduced level of functionality in the measured area and is somewhat capable of providing the requested output.
- Low (1) – The tool is able to provide limited to no functionality in the measured area and is not capable of providing the requested output.

	DopplerVue	What's Up Gold	Solar Winds	DopplerVue	What's Up Gold	Solar Winds
Utilization and Error Rates						
Consistent Performance Rates						
Performance Data Collection						
Performance Data Analysis						
Problem Reporting						
Performance Data and Statistics Collection						
Average Score						

Table 2. Performance matrix table

Each of the three categories will be assigned a numeric value of one to three. This numeric value will then be used to calculate an application's average, which will serve as a measure of the tools functionality. Therefore, the tool with the highest average has the greatest functionality and consequently is considered the best tool for network management.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. LABORATORY AND NETWORK RESEARCH

A. TNT EXPERIMENT TESTBED

1. History

The development of TNT experiments can be traced to FY02 when Unmanned Arial Vehicles (UAV) were explored as a means to assist in downed pilot rescue missions. In January 2003, these experiments merged with the Surveillance, Targeting, and Acquisition Network (STAN) and in July of the same year quarterly experiments began. The STAN experiments evolved into what is now TNT; through progressive quarterly experiments, TNT tests both mature and immature information and other technologies and their application to SOCOM missions. In addition, TNT is the basis for the formation of the Center for Network Innovation and Experimentation, a research center formed in 2005, which partners NPS, Lawrence Livermore National Laboratory (LLNL), SOCOM, and other agencies (Haines, 2006).

2. CENETIX

CENETIX is based aboard NPS in Monterey, California, and maintains the CENETIX Lab. Through the efforts of NPS faculty, staff, and students, CENETIX implements an 802.16 Orthogonal Frequency Division Multiplexing (OFDM) wireless network connecting CENETIX facilities within the Monterey Area to experimentation facilities located approximately one hundred miles South at the Camp Roberts, California, Army National Guard Base.

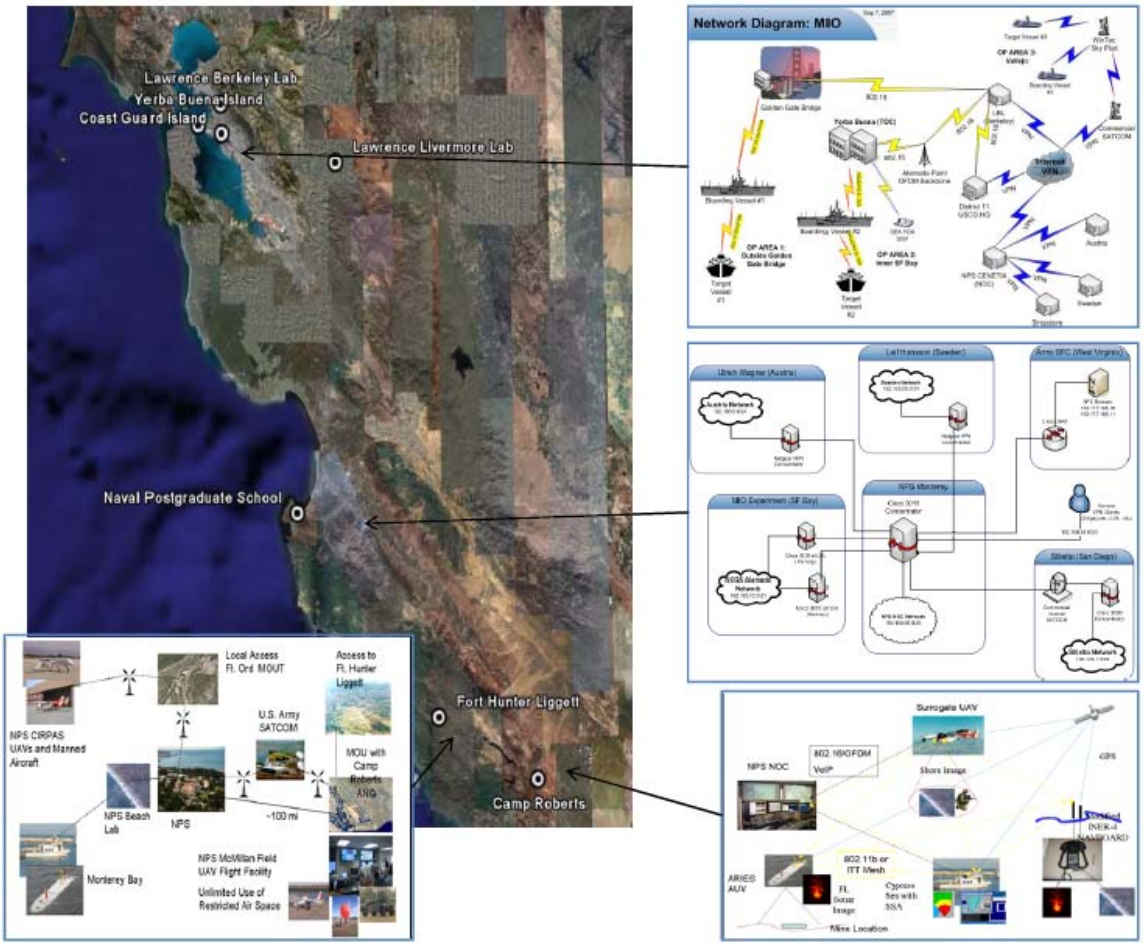


Figure 7. Diagram of CENETIX Network (After: Bordetsky and Clement, CENETIX LAB 2007)

These backbone connections of the network, along with facilities at the Monterey laboratory, the Center for Interdisciplinary Remotely Piloted Aircraft Studies (CIRPAS) in Marina, California, Fort Hunter Liggett, the Military San Francisco Bay, and Avon Park, Florida, along with additional ground, air, and maritime locations, allow for a collaborative testbed that provides a multi-theater Command and Control (C2) structure supporting missions and objectives of the CENETIX research team. Figure 7 depicts the CENETIX network backbone. The overall mission is to

support advanced studies of wireless networking with unmanned aerial, underwater, and ground vehicles in order to provide flexible deployable network integration with an operating infrastructure for interdisciplinary studies of multiplatform tactical networks, GIG connectivity, collaborative technologies, situational awareness systems, multi-agent architectures, and management of sensor-unmanned vehicle-decision maker self-organizing environments (Haines, 2006).

B. SOFTWARE AND EQUIPMENT

1. Monitoring Tools

There is an abundance of commercial and open-source network management tools, offering a variety of option and capabilities to manage networks. The intention of this experiment is not to provide a comprehensive listing of performance monitoring tools but rather to provide an overview of three specific tools made available by three separate commercial vendors, and to extrapolate the lessons learned/results onto other tools. Specifically, SolarWinds and What's Up Gold were selected based on limited personal field experience and existing government contracts; DopplerVue was selected as part of a continued CENETIX evaluation effort. Although not a monitoring tool evaluated as part of this thesis research Wireshark was selected to assist in the analysis of network packet data.

SolarWinds Orion Network Performance Monitor provides a variety of network management solutions ranging from individual monitoring tools to complete, full-featured monitoring platforms. Orion is a comprehensive monitoring solution built on SNMP. The Orion management application

features a web interface with real-time monitoring of availability, bandwidth utilization, network latency and many other network performance metrics. The current version of SolarWinds is not configured to monitor IPv6; however, the unreleased upgrade software is expected to address IPv6 management requirements. For the purpose of this thesis, SolarWinds will be solely used as comparison model on IPv4 network performance management.

Ipswitch WhatsUp Gold MSP Edition v12 (commercial product) is a graphical network monitoring system designed for multi-protocol networks. Its vector-based graphics and map diagramming features allow users to customize network maps according to their needs; Log Manager and advanced network device discovery enables users to navigate through event data and pinpoint specific problems in order to perform the necessary corrective actions. The SNMP Viewer allows network administrators to troubleshoot problems in real-time as well as track historical performance data to better manage networks. It provides mapping, miniaturization, notification, and information of yield of networks for quick detection and monitoring of critical devices.

DopplerVue (commercial product) is a next-generation self-aware network management tool, integrating fault and performance with discovery and automated mapping into a single unified dashboard across devices, applications, and services. This product is able to connect to other IP-enabled devices, services and applications through SNMP, SYSLOG and Window Management Instrumentation (WMI) to provide integrated Fault and Performance monitoring.

WireShark, formerly known as Ethereal, is an open source packet capture tool for Ethernet networks designed to capture all traffic passed over a network when the network interface card is placed in promiscuous mode, provided the traffic desired is visible on that given interface. Although WireShark does not calculate performance statistics on captured traffic, it does permit analysis of individual packets, by displaying the time, packet number, source and destination IP address, as well as protocol used during any given conversation. The ability to filter packets based on protocol as well as other characteristics such as IP address and port number helps narrow the focus of desired captured data. The tool's capture library enables WireShark to capture and save packets off the network interface while a graphic user interface allows administrators to view and analyze captured packets.

2. Software Application

Numerous software applications have been incorporated into the monitoring desktop computers to maintain and monitor the network and to provide for mission essential needs. This section gives a brief explanation of the software suite. Table 3 lists the individual software applications currently in use within the network monitoring computers.

Hardware	Software	**Remarks**
Dell Desktop #1	Microsoft Window XP Pro SP2 (Operating System)	Common operating system (OS) utilized throughout DoD. This OS is compatible with numerous applications being operated throughout TNT network.
Dell Desktop #2	Microsoft Window VISTA (Operating System)	Common operating system (OS) utilized throughout commercial mark but not yet approved for usage within DoD. This OS is preset for full compatibility with IPv6.
Dell Desktop #1 and 2	Microsoft Server SQL 2005 Express	Is a relational database management system (RDBMS) with the primary query language being Transact-SQL, an implementation of the ANSI/ISO standard Structured Query Language (SQL) used by both Microsoft and Sybase.
Dell Desktop #1 and 2	ASP.Net Framework 2.0	ASP.NET is a web application framework developed and marketed by Microsoft, that programmers can use to build dynamic web sites, web applications and web services.
Dell Desktop #1 and 2	Internet Explorer 7	Microsoft Window web browser.

Table 3. Supporting softwares

a. Dell Desktop Optiplex GX2270

The Dell Optiplex GX270 was chosen due to availability as well as its current use by many DoD institutions. The two desktops, each running a different OS, are located within the NPS CENETIX lab. The purpose of the two desktops is to capture all active nodes within the TNT experimentation network and to manage/monitor node performance.

Windows XP Professional with Service Pack (SP) 2 is installed on desktop #1 and configured as an IPv4 client with IPv6 enabled. The operating system running on desktop #2 is Windows Vista and is IPv6 enabled.

Figure 8. Two Dell GX270 desktop setup

b. Windows XP Pro SP2

Windows XP is an operating system developed by Microsoft Corporation and released in October 2001. Windows XP was designed to deliver a fresh user-interface while merging two of their premier operating systems, Window NT and Windows ME. Desktop #1 is configured with Windows XP Professional SP2 edition to operate primarily utilizing IPv4 however since the release of SP2 in early 2007 support for IPv6 has been added.

c. Windows Vista

Like Windows XP, Vista is also an OS produced by Microsoft and released in January 2007. As part of the networking architecture redesign, IPv6 is incorporated into

the operating system (Figure 8), along with a number of performance improvements such as TCP window scaling. Windows Vista includes more comprehensive support for wireless networking, in comparison to previous versions of Windows.

d. Supporting Applications

A key requirement for operating DopplerVue was the installation of Microsoft Server SQL 2005 Express, and ASP.NET v2.0 or greater. DopplerVue requires both to generate topology diagrams while actively monitoring the network and managing program runtime over web applications. Depending on the size of the network, the upgraded version of SQL Server 2005 may be required for larger network setup.

3. Service Router – Cisco 2811

The Cisco 2800 series integrated service routers (2801, 2811, 2821, and 2851) are a spin off from the 2600 series. According to manufacture specifications, this series supports Layer 2 switching with Power over Ethernet (PoE), high-density serial connectivity, enhanced network analysis, and traffic management tools. These routers also offer such improvements as embedded security processing and new high-density interfaces. The high-density interfaces in particular, heighten the performance, availability, and reliability required for scaling missions. In addition, Cisco 2800 series routers have functionality that support wireless LANs. Specifically, they support WLAN coverage, providing wireless capabilities combined with routing and security features in a single device (Stewart, 2006).

Feature	2801	2811	2821	2851
Form Factor	1 RU	1 RU	2 RU	2 RU
Integrated Routed/WAN Ethernet	2 10/100	2 10/100	2 10/100/1000	2 10/100/1000
10/100 Ethernet Switch Ports	Up to 16	Up to 32	Up to 40	Up to 64
Broadband WAN Support	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC	Optional ADSL and G.SHDSL HWICs, DOCSIS 2.0 HWICs, and 3G HWIC
Interface Card Slots	2 HWIC/WIC/VIC/VWIC 1 WIC/VIC/VWIC 1 VIC/VWIC	4 HWIC/WIC/VIC/VWIC	4 HWIC/WIC/VIC/VWIC	4 HWIC/WIC/VIC/VWIC
Embedded Crypto Processor	Yes	Yes	Yes	Yes
Default/Max Flash	64/256 MB	64/256 MB	64/256 MB	64/256 MB
Default/Max SDRAM	128/384 MB	256/768 MB	256/1024 MB	256/1024 MB
Cisco Router and Security Device Manager (SDM)	Yes	Yes	Yes	Yes
IPv4 Routing Protocols	RIP v1/v2, EIGRP, OSPF, BGP, PBR, and PfR	RIP v1/v2, EIGRP, OSPF, BGP, PBR, and PfR	RIP v1/v2, EIGRP, OSPF, BGP, PBR, and PfR	RIP v1/v2, EIGRP, OSPF, BGP, PBR, and PfR
Multicast Routing Protocols	PIM-SM, mroute (static route), and MLD	PIM-SM, mroute (static route), and MLD	PIM-SM, mroute (static route), and MLD	PIM-SM, mroute (static route), and MLD
IPv6 Routing Protocols	EIGRP, RIPng, OSPFv3, IS-IS, and PBR	EIGRP, RIPng, OSPFv3, IS-IS, and PBR	EIGRP, RIPng, OSPFv3, IS-IS, and PBR	EIGRP, RIPng, OSPFv3, IS-IS, and PBR
Stateful Firewall	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image	Yes, requires Advanced Security and up Cisco IOS Image
Integrated 802.11 b/g Access Point	HWIC (optional)	HWIC (optional)	HWIC (optional)	HWIC (optional)
Integrated 802.11 a/b/g Access Point	HWIC (optional)	HWIC (optional)	HWIC (optional)	HWIC (optional)
RP-TNC Connectors for Field-replaceable Optional High-gain Antennas	Yes	Yes	Yes	Yes
Diversity (Dual) Antennas	Yes	Yes	Yes	Yes
Wireless LAN Controller Module	—	6, 8, 12 802.11a/b/g/n AP controller	6, 8, 12 802.11a/b/g/n AP controller	6, 8, 12 802.11a/b/g/n AP controller

Figure 9. Comparison of Cisco 2800 Series Integrated Model (After: Cisco System)

One of the key factors that makes this device a viable part of experiment is its ability to support both IPv4 and Ipv6 routing protocols and multicast routing protocols.

C. PROTOCOLS

1. Simple Network Management Protocol (SNMP)

First defined in RFC 1098 of 1989, Simple Network Management Protocol (SNMP) was designed to provide a low-overhead base for multivendor network management of

routers, servers, workstations, and other network resources (Gateau, 2007). RFC 1098 was later updated in RFC 1157 in 1990 and is now known as SNMPv1. SNMP was further improved by RFC 3416, 3417, and 3418 to become what is now known as SNMPv2, and in 1999 SNMPv3 was specified in RFC 2570 (Mauro et al, 2005).

As outlined by William Stallings the network management model used for SNMP consists of the following:

- Management Station
  - the interface for the human network manager into the network management system.
- Management Agent
  - key platforms (hosts, bridges, routers, and hubs) equipped with SNMP agent software to facilitate management by the management station.
  - responds to requests for information, and
  - requests for action from the management station.
  - May provide management station important but unsolicited information
- Management Information Base (MIB) –
  - collection of access points used by the management station to access the agent.
  - Maintained by the agent software.
  - Is standardized across systems of a given class
  - Can be modified by proprietary extensions

MIB values are retrieved by the management station(s) performing the monitoring function and can make an agent act as desired or change configuration settings by modifying values of specified variables.

Furthermore, SNMP links the management station(s) to its agents utilizing the User Datagram Protocol (UDP) because it is connectionless and allows the management

station(s) to communicate with agents without creating an end to end connection. This link then makes management information available for transfer or modification through three commands. A management stations uses the *get* command to retrieve status information from an agent and will receive a *getresponse* message in response. The *set* command is used to modify agent parameters and the *trap* command allows the agent to send unsolicited messages to the management station(s). The table below outlines SNMP operations and the versions supported by each.

Name	Minimum SNMP Version
get	1
getnext	1
getbulk	2
set	1
getresponse	1
trap	1
notification	2
inform	2
report	3

Figure 10. SNMP operations (From: Gateau, 2007)

2. Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) produces message packets to report errors and other information regarding IP packet processing back to the source (Cisco, 2005). ICMP is the primary signaling mechanism for IP and is required in its basic form by every IP implementation (Goswami, 2003). ICMP messages are sent for a variety of reasons and include: when a datagram cannot reach its intended destination, when the gateway does not have the buffering capacity to forward a datagram, or when a gateway

router is able to direct the host to send traffic on a shorter route. Each of these reasons will generate a message that can be categorized into one of the following message types, Destination Unreachable, echo Request and Reply, Redirect, Time Exceeded, Router Advertisement, and Router Solicitation. Each message type has a corresponding numeric Type Field assigned to help identify the message. Figure 11 represents a list of ICMP messages and corresponding Type Fields.

TYPE	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect Message
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request
18	Address Mask Reply

Figure 11. ICMP messages and assigned Type Fields (From: Help&Support, No Date Given)

Destination Unreachable can be further divided into four basic types:

- network unreachable – typically means a failure has occurred in the routing or addressing of a packet.
- host unreachable – indicates a delivery failure, i.e. wrong subnet mask.
- protocol unreachable – means that the destination does not support the protocol specified in the packet.
- port unreachable – implies the TCP socket or port is not available.

Like the Type Field assigned to each message, each of the Destination Unreachable messages, as outlined above, is assigned a numeric code that helps further describe the problem. Codes 0,1,4, and 5 may be received from a gateway; and codes 2 and 3 may be received from a host (Postel, 1981).

Codes	
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service

Figure 12. Destination Unreachable message and correspondence codes (From: ICMP, No Date Given)

The ICMP echo-request is generated by the ping command and sent by any host to test node reach ability. In response, the host initiating the contact will receive an echo-reply indicating that the desired node can be successfully reached. Otherwise known as *ping* the successful exchange between an echo-request and reply verifies that major pieces of the transport system work (Comer, 2000).

An ICMP Redirect message is sent by the router to the source host to provoke more efficient routing (Cisco, 2005). The router will still forward the original packet

to its intended destination. Redirect allows for host routing table to remain small, since the host is only required to know the address of one router. Although routing tables are kept small optimal routes for all destinations in use are also maintained. Redirect messages are sent by the router only when the host sends a packet for which there is a better route available.

The ICMP Time-exceeded message is sent by a router when the Time-to-Live (TTL) field, of a packet, reaches zero. Time-to-Live is expressed in hops or seconds. The TTL field keeps packets from repeatedly looping, given the network contains a routing loop. Once TTL reaches zero the packet is discarded and Time-exceeded message is returned to the source host.

D. EXPERIMENTATION

1. TNT 08-03

During TNT 08-02, a direct IPv6 link was set and tested using an IPv6 enabled UAV node (Figure 13).

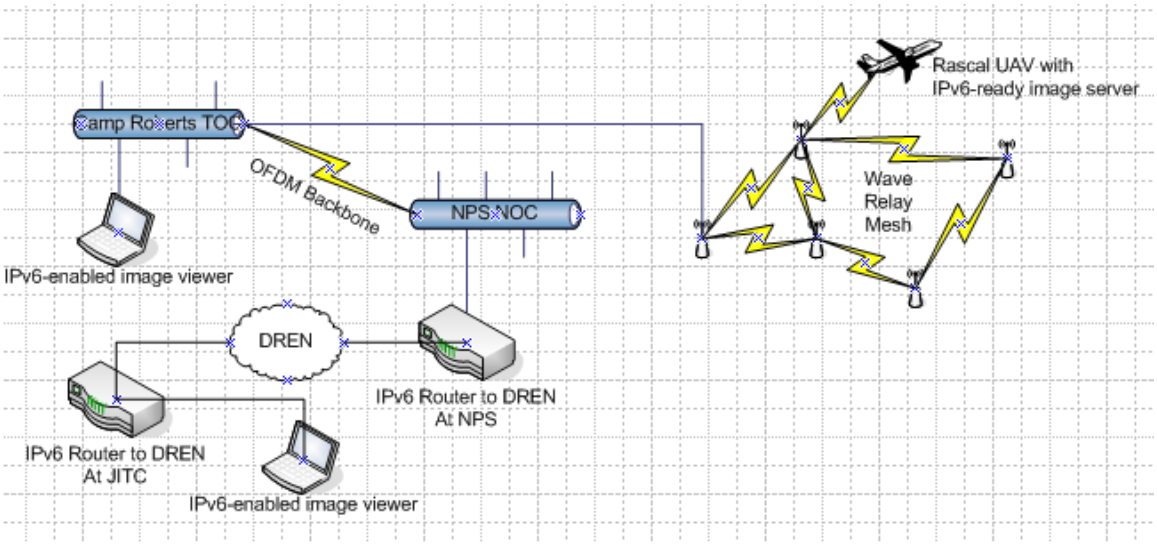


Figure 13. TNT 08-02 IPv6 UAV link topology

This experiment was highly successful in feeding live video directly from the Rascal UAV through the OFDM backbone and ultimately to the Joint Interoperability Testing Command (JITC) IPv6 gateway. TNT 08-02 experimentation provided evidence that tactical sensor nodes can be configured with IPv6 devices, and successfully pass video over a hybrid network.

Continuing from the previous experiment, TNT 08-03 takes a look at network management of tactical IPv6 nodes with a concentration on performance management. In addition to monitoring the Rascal UAV the Light Reconnaissance Vehicle (LRV) was incorporated as an additional IPv6 sensor on-the-move node. The IPv6 sensor node was installed on board the LRV, located at Camp Roberts, and configured to transmit video and data packets. During this experiment the CENETIX Network Operations Center (NOC) housed the management components. Two Dell desktop computers; each configured to support both IPv4 and IPv6 had network management applications WhatsUp Gold and DopplerVue installed.

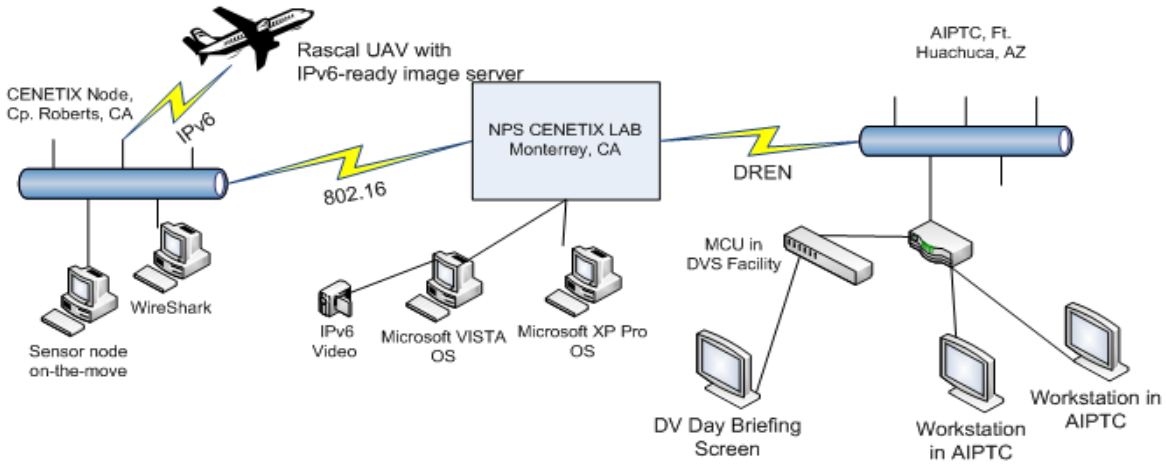


Figure 14. TNT Architecture IPv6 TNT 08-03

The overall objective of TNT 08-03 experimentation was to evaluate the ability of WhatsUp Gold, DopplerVue and SolarWind to monitor a network with tactical IPv4 and IPV6 sensor nodes.

2. Observation

It is well understood that all three software DopplerVue, WhatsUp Gold and SolarWind (later dropped due to IPv6 incompatibility issue) have exemplified and demonstrated their ability to accurately manage and monitor IPv4 networks. Therefore, this thesis will primarily focus only on network performance management of IPv6 nodes.

a. Initial Look

The initial configuration of both DopplerVue and What's Up Gold was set per each vendor's specification as outlined in their user's guide. Both applications were preconfigured to auto-discovery mode for both IPv4 and IPv6 nodes using ICMP, HTTP and SNMP protocols. In DopplerVue, the auto-discovery mode was accomplished by presetting all network elements within the specified IP address range: IPv4 ranges were from 192.168.99.01 to 255 and IPv6 range were from 2001:480:211:1100::01 to 255. This specific range was selected based on known IP assignments and allowed research efforts to be concentrated on known active devices. The narrow range selected facilitated research, despite having a similar active discovery mode What's Up Gold requires the administrator to manually enter known IPv6 addresses one by one. This can be a potential management problem when dealing with networks consisting of large numbers of active IPv6 nodes. For example, if the

range used was 2001:480:211:1100::01 to 2001:480:211:1100:FFFF:FFFF:FFFF:FFFF every possible IP address would have been accounted for, but would make for an insurmountable research problem given the time required to enter each individual IP address. Both applications immediately provided topology consisting of all the active nodes within the TNT network as shown below in Figure 15 and 16.

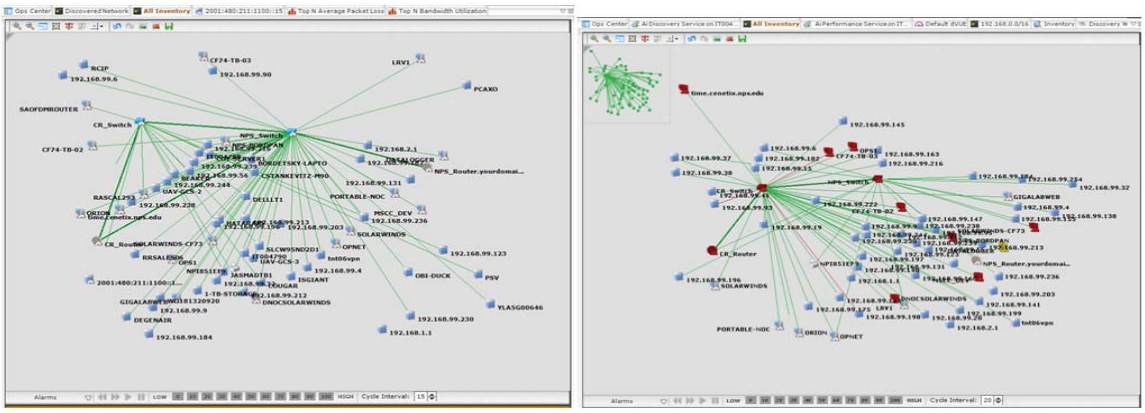


Figure 15. DopplerVue, left Vista and right XP Pro, topology view of active nodes within the TNT network

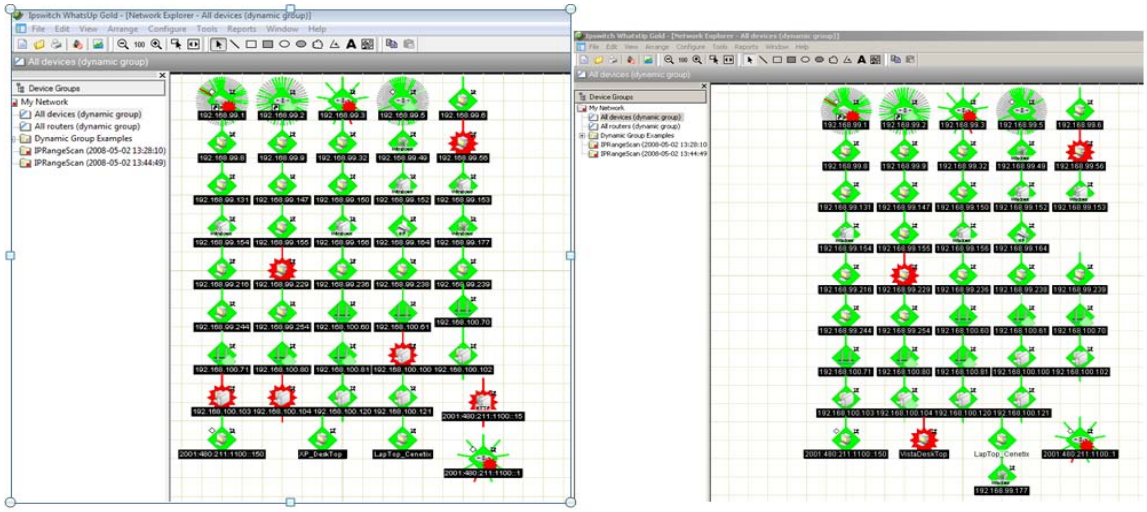


Figure 16. WhatsUp Gold, left Vista and right XP Pro, topology view of active nodes within the TNT network

Both applications were pre-configured by the manufacture to provide real time network performance metric reports. Below, Table 4 breaks down the types of report generated by each network management (NM) application.

DopplerVue PM Reports	**WhatsUp Gold PM Reports**
All Nodes Discovered	Group Health
Interface Bandwidth Utilization	Disk Utilization
Link Status	CPU Utilization
Router and Interface Details	Ping Gauge
Top N Average CPU Utilization	Interface Utilization
Top N Average Latency	Memory Utilization
Top N Average Packet Loss	State Summary
Top N Bandwidth Utilization	Ping Availability/Response Time
Top N Most Recent Discovered	Top 10 General Status Report

Table 4. Type of reports generated by network management application

Due to technical difficulties, the LRV was ineffective and did not participate in the experiment. During the UAV (Rascal) portion of the experiment, both applications were configured to search for Rascal, which was configured as an IPv6 node. Both devices failed to detect the Rascal's IPv6 address (2001:480:211:1100::15) through the automated polling command. Even, when Rascal's IPv6 address was manually entered into each application, DopplerVue on the XP Pro platform still failed to detect the Rascal. Figure 17 shows WhatsUp Gold Vista actively monitoring both IPv4 and IPv6 packets.

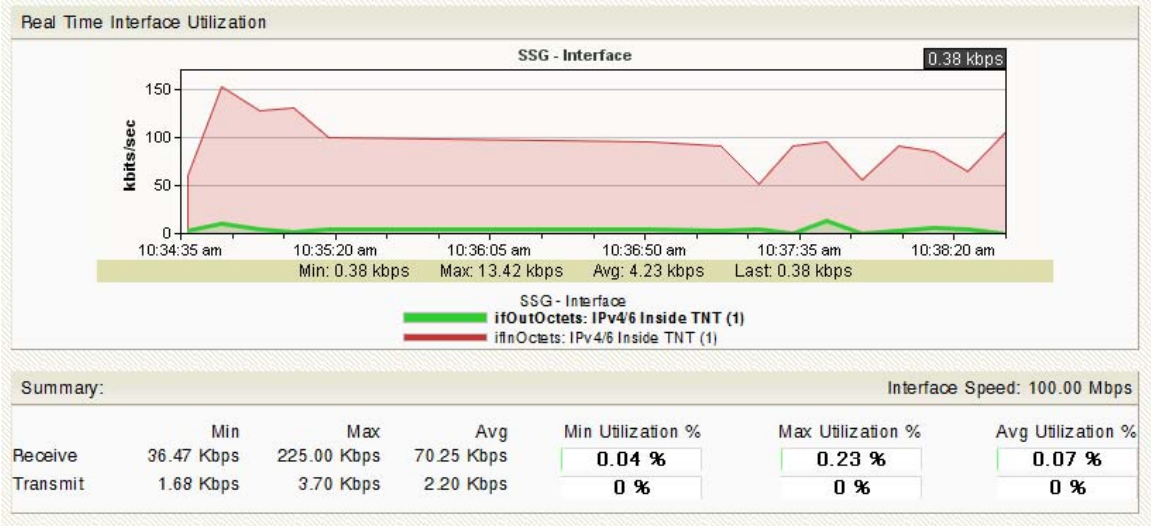


Figure 17. WhatsUp Gold Vista platform monitoring IPv4 and IPv6

WhatsUp Gold on both Vista and XP Pro platforms were able to detect Rascal's IPv6 address, but only Vista's WhatsUp Gold was able to actively monitor network performance using Internet Control Message Protocol (ICMP) ping (Figure 18).

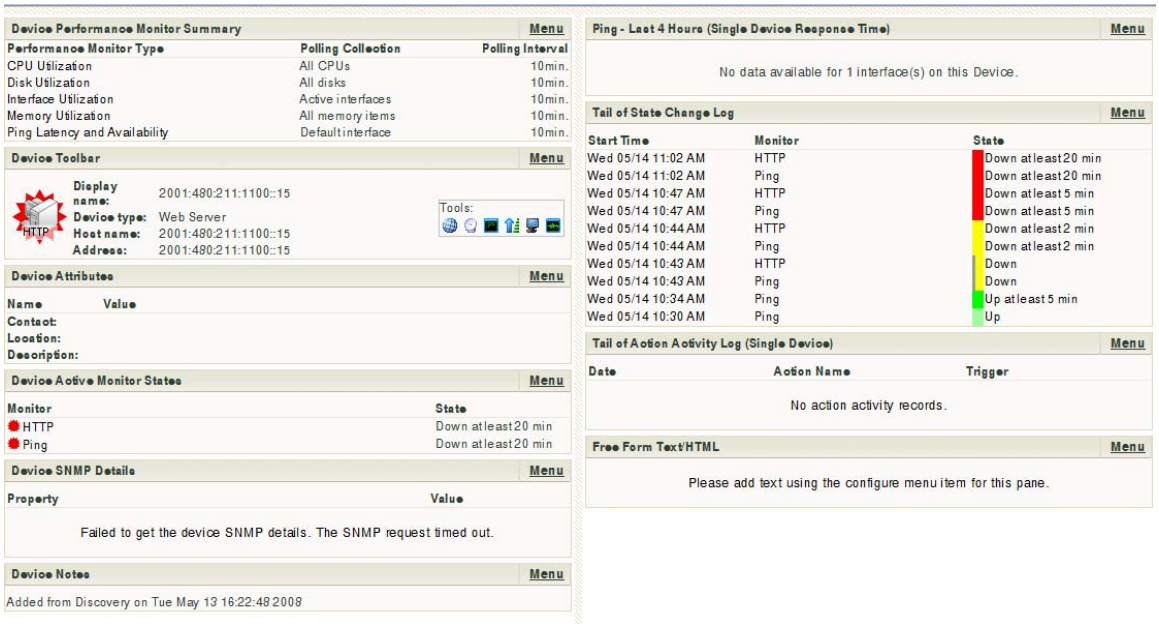


Figure 18. IPv6 Rascal's performance monitoring on WhatsUp Gold Vista Platform

As for DopplerVue, only the Vista platform was able to maintain active network monitoring using SNMP and ICMP ping as shown in Figure 19.

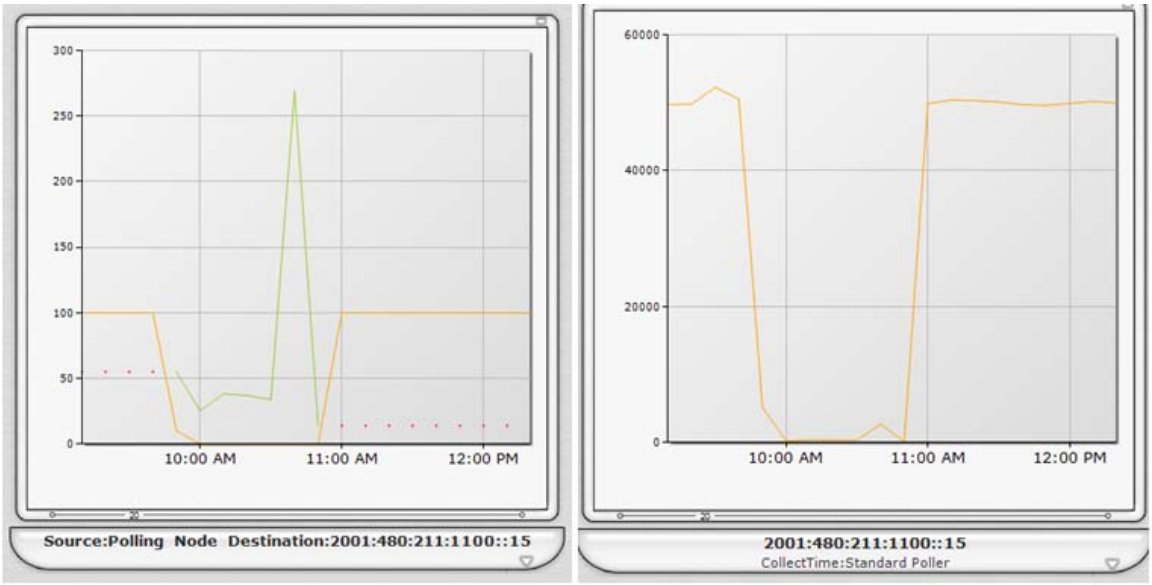


Figure 19. Active Ping from DopplerVue Vista of Rascal IPv6 node

Additional tests were performed to evaluate the reliability of both applications by performing a trace route of the Rascal node. Both DopplerVue and WhatsUp Gold on the Vista platform were able to actively trace Rascal routes.

b. Observation and Key Issues

As mentioned in the previous section, the applications installed on the XP Pro SP2 platform failed to provide real-time monitoring of the desired IPv6 node. This may be due to XP's manufacturer configuration setting IPv4 as its primary IP protocol encapsulating IPv6. At a glance, the resulting IPCONFIG output, as displayed in Figure 20, may seem a bit overwhelming. However, what

needs to be understood is that when IPv6 is enabled the protocol automatically assigns an IP to every interface. Furthermore, each interface is assigned an IP depending on its intended purpose (Hagen, 2006); Figure 20 displays global IP, link local, and site local addresses assigned to the platforms multiple interfaces. In RFC 2462, S. Thompson and T. Narten define the previously mentioned types of addresses as follows:

- link-local address - an address having link-only scope that can be used to reach neighboring nodes attached to the same link. All interfaces have a link-local unicast address.
- site-local address - an address having scope that is limited to the local site.
- global address - an address with unlimited scope.

A link local address compares to private IP addressing in IPv4 and is derived by combining the prefix fe80::/64 with the Ethernet MAC address assigned to a given interface. Because every MAC is unique no two interfaces will have the same IP. Similarly, what is referred to as a site-local address in IPv4 is known as unique local IPv6 unicast address or local IPv6 address and is specified in RFC 4193 (Hagen, 2006). The Internet Assigned Numbers Authority (IANA) has assigned the FC00::/7 prefix to "Unique Local Unicast" (Hinden et al, 2005). Addresses with the prefix FDOO::/8 represent locally administered addresses which also fall under the local IPv6 address domain as do those starting with the prefix FEC0; however, FEC0 is a remnant of older implementations that should no longer be used. An IPv6 global address starts with the

prefix 2000::/3 as specified in RFC 3513 and is like the IPv4 public address used to access the internet.

More specifically, IP addresses in Figures 20 and 21 starting with 2001 are representative of global addresses connecting the Defense Research and Engineering Network (DREN) and the CENETIX lab via the internet. Addresses beginning with fd00 are representative of the connection between Science Applications International Corporation (SAIC) and the CENETIX lab; and those beginning with fe80 represent intranet connections.

The key observation is the large number of IPv6 addresses assigned to the XP OS platform. Unable to determine why so many similar addresses are assigned to a single platform it is assumed that Figure 20 is a true representation of all active interfaces on the platform. What effect so many addresses assigned to this single platform have on add-on network management applications is not currently known but may explain the inability to actively monitor and provide real-time data on IPv6 nodes. Further research into this matter may justify above the assumption.

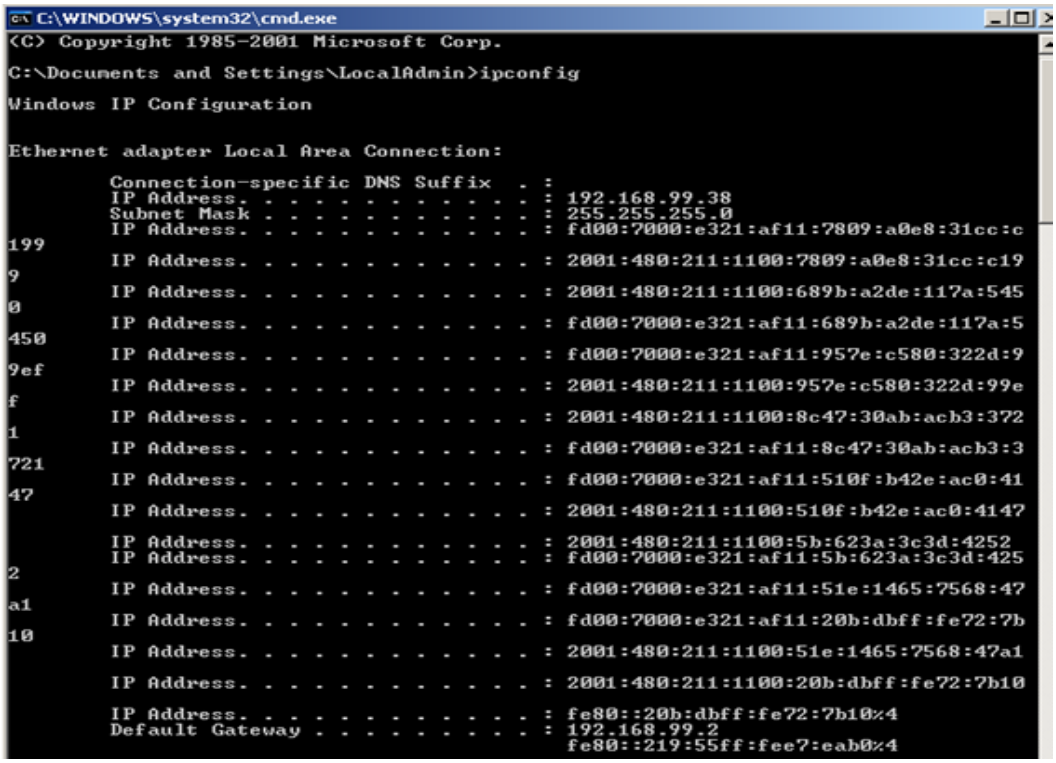


Figure 20. Ipconfig view of Dell desktop installed with Windows XP SP2 OS

Unlike XP Pro, Windows Vista OS' primary IP protocol is IPv6 followed by IPV4 as the secondary as shown in Figure 21.

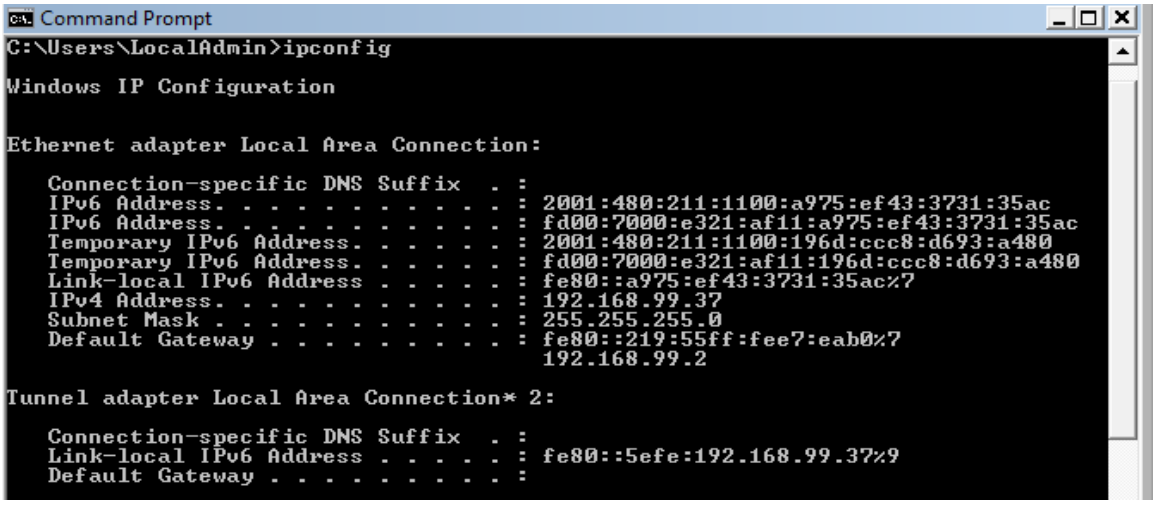


Figure 21. IPconfig view of Dell desktop installed with Windows Vista OS

Both applications (DopplerVue and WhatsUp Gold) were able to provide real-time live data on the Rascal, however, neither application was able to actively seek and detect IPv6 nodes without human intervention. For DopplerVue, the administrator is required to manually predefine the range of IPv6 addresses, whereas WhatsUp Gold, only allows for entry of one IPv6 address at a time. Currently, there is no other feasible way of entering multiple IPv6 addresses into WhatsUp Gold (Donnelly, 2008).

Throughout the experiment, each NM application provided some relevant and useful data pertaining to the health of Rascal node. For example, during Rascal's flight, DopplerVue was able to provide few graphical performance monitoring pictorials such as packet loss, latency, discovered status and alarm reports. Likewise WhatsUp Gold, provided ping availability, state change timeline, health, and utilization reports.

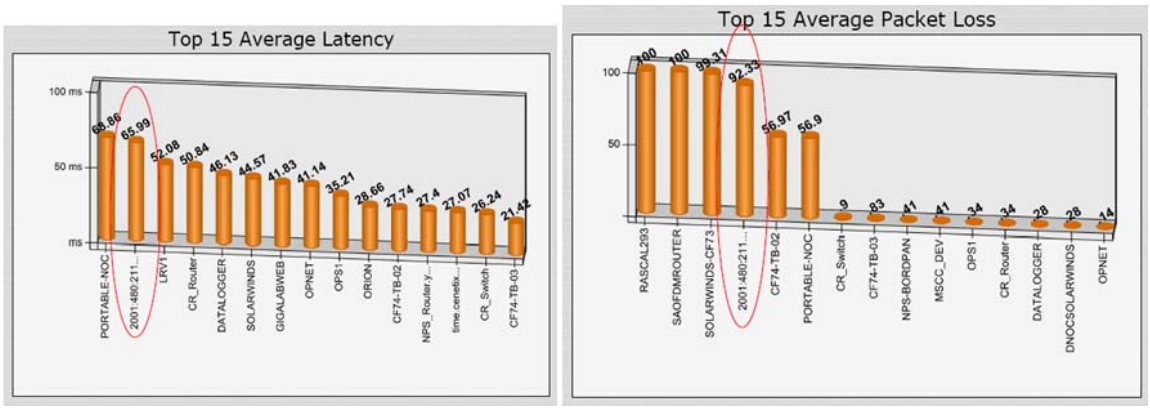


Figure 22. DopplerVue Vista of IPv6 data captured, TNT 08-03

Beyond the mentioned report, both failed to provide any in depth analysis of actual health and usability of the Rascal node, such as ability to see route paths to other IPv6

connections, trends in traffic load and bandwidth availability for each active node. Overall, both applications provided basic IPv6 performance data but lack the ability to truly manage tactical IPv6 nodes. TNT 08-03 experiments revealed there are many legacy systems within the network as well as software that may prevent the selected applications to truly acquire and manage IPv6 devices. It is painfully obvious that until commercial vendors are willing to fully support both IPv6 and IPv4 our job as network managers will be increasingly more difficult.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATION

A. CURRENT STATE OF TECHNOLOGY

The implementation of IPv6 is a revolutionary event requiring dedicated attention in all areas, specifically network management. TNT 8-03 experimentation proves, albeit at a very rudimentary level, that network management tools currently on the market do not provide enough IPv6 support. When network management applications require human intervention to assist in the discovery of new nodes or devices their intended purpose is minimized, resulting in decreased usefulness. A network that cannot monitor and manage its own nodes is no better than an unsecured network (Jilong, 2004). Given the nature of SOCOM's mission it is imperative that network management applications are capable of monitoring each and every device that enters their domain, whether friendly or foe. The inability to provide such a function leaves tactical nodes vulnerable to both insider and outsider attacks. Whether intentional or unintentional these attacks can potentially render a mobile node's ability to communicate ineffective.

To truly measure an applications ability to perform and provide useful and relative data it must be tested in an environment mirroring that in which it will most likely be utilized. TNT 08-03 serves as a stepping stone and has resulted in an enhanced understanding as to what each of the chosen network management applications are capable of doing and providing. It is hard to concretely determine, without further study, if the results are due to manufacturer configuration, OS incompatibility, or simply a

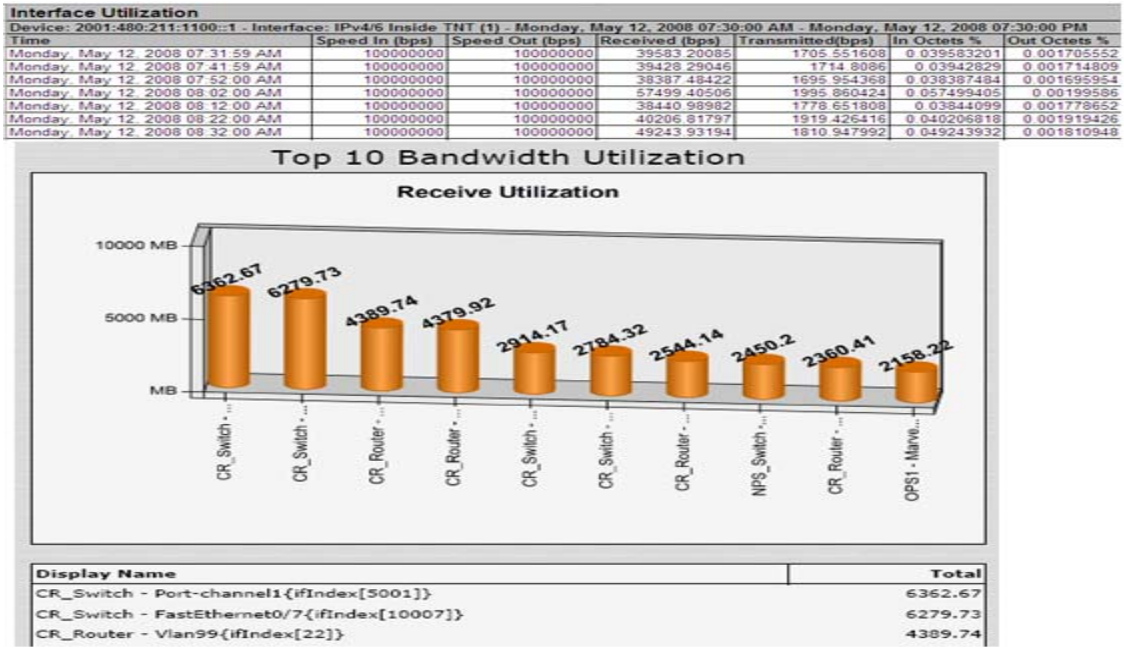
result of operator error and application misconfiguration. However, given the results it is apparent that Windows XP Pro, designed for IPv4, does not handle IPv6 node management very well as seen in below Figure 23.

	Vista Platform			XP Platform		
	DopplerVue	WhatsUp Gold	Solar Winds	DopplerVue	WhatsUp Gold	Solar Winds
Utilization and Error Rates	0	0	0	0	0	0
Consistent Performance Rates	0	1	0	0	0	0
Performance Data Collection	2	2	0	0	1	0
Performance Data Analysis	0	0	0	0	0	0
Problem Reporting	0	1	0	0	0	0
Performance Data and Statistics Collection	1	1	0	0	0	0
Average Score	**0.5**	**0.8**	**0**	**0**	**0.2**	**0**

Figure 23. Results on network management tools

Based on pre-established metrics from Chapter three, WhatsUp Gold received rating of 0.8, DopplerVue 0.5 and SolarWind zero. What made WhatsUp Gold more usable within network management aspect was its ability to provide detail analysis reports, whereas DopplerVue provided generic values. However, the key factor was its ability to maintain monitoring of IPv6 sensor on the move node (Rascal). Following are the justification behind the grading:

- *Utilization and Error Rates*: Both WhatsUp Gold and DopplerVue, Figure 24, lacked an ability to collect Rascal's utilization rate, however, WhatsUp Gold was able to detect and monitor Cisco's router in IPv6 address form. This is indicative of WhatsUp Gold's ability to recognize both IPv4 and IPv6 protocols on same device. What cannot be determined from the output is whether the traffic generated by the Rascal is enough to register in either WhatUp Gold or DopplerVue. When packet captures on Wireshark are filtered using the Rascal's IPv6 address the following output is provided.



Interface Utilization

Device: 2001:480:211:1100::1 - Interface: IPv4/6 Inside TNT (1) - Monday, May 12, 2008 07:30:00 AM - Monday, May 12, 2008 07:30:00 PM

Time	Speed In (bps)	Speed Out (bps)	Received (bps)	Transmitted(bps)	In Octets %	Out Octets %
Monday, May 12, 2008 07:31:59 AM	100000000	100000000	39583.20085	1705.551608	0.039583201	0.001705552
Monday, May 12, 2008 07:41:59 AM	100000000	100000000	39428.29046	1714.8086	0.03942829	0.001714809
Monday, May 12, 2008 07:52:00 AM	100000000	100000000	38387.48422	1695.954368	0.038387484	0.001695954
Monday, May 12, 2008 08:02:00 AM	100000000	100000000	57499.40506	1995.860424	0.057499405	0.00199586
Monday, May 12, 2008 08:12:00 AM	100000000	100000000	38440.98982	1778.651808	0.03844099	0.001778652
Monday, May 12, 2008 08:22:00 AM	100000000	100000000	40206.81797	1919.426416	0.040206818	0.001919426
Monday, May 12, 2008 08:32:00 AM	100000000	100000000	49243.93194	1810.947992	0.049243932	0.001810948

Display Name	Total
CR_Switch - Port-channel1{ifIndex[5001]}	6362.67
CR_Switch - FastEthernet0/7{ifIndex[10007]}	6279.73
CR_Router - Vlan99{ifIndex[22]}	4389.74

Figure 24. WhatsUp Gold (top) and DopplerVue (bottom) Utilization Report, TNT08-03

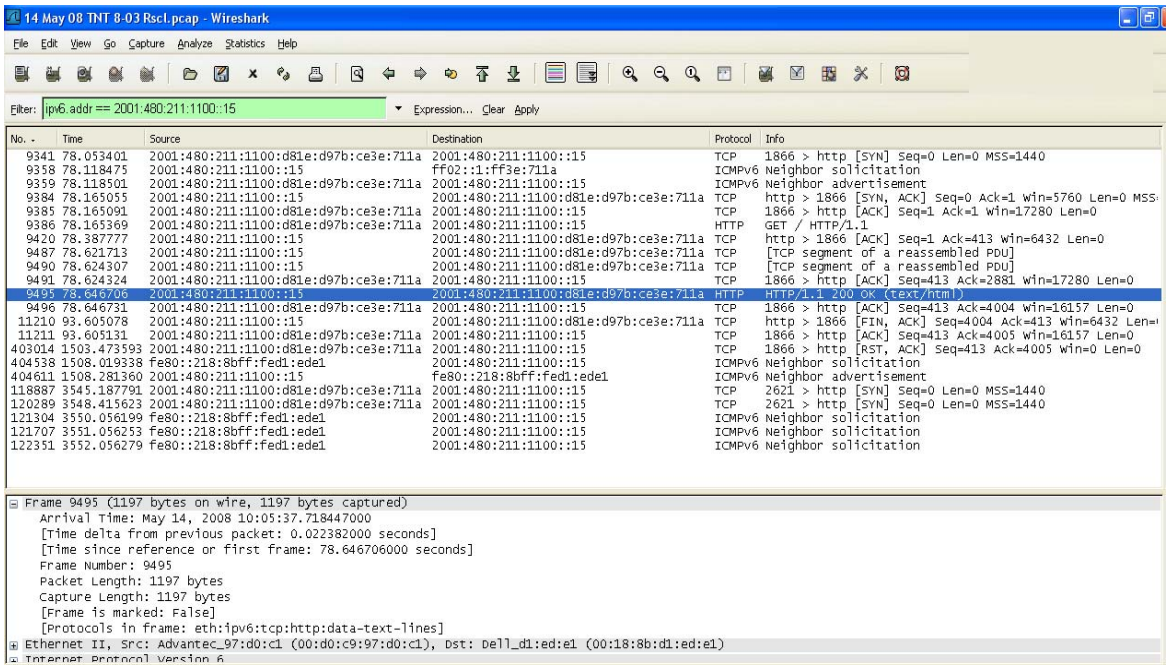
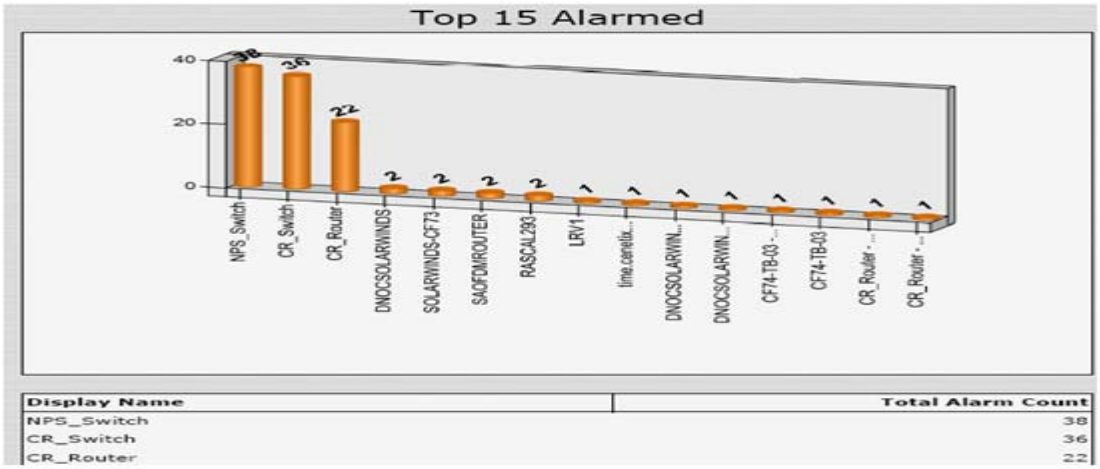


Figure 25. WireShark data collection TNT03-08

The highlighted packet in Figure 25, number 9495, is the largest at 1197 bytes and is representative of the Rascal's connectivity and communication with its file server. Perhaps, a small and seemingly insignificant amount of traffic but one that should be captured by DopplerVue given it is able to register when there is no traffic being transmitted over a given link as evidenced by the zeros registered in the Group Interface Report above.

- *Consistent Performance Rate*: WhatsUp Gold was able to provide a limited performance data report on Rascal, called Group Health. The Group Health report provides method of monitoring, state of connection and duration. DopplerVue lacks the capability to produce a report that captured Rascal's performance rate consistently over time.
- *Performance Data Collection*: Both NM tools provide some means of performance data collection through SNMP and ICMP. DopplerVue and WhatsUp Gold were able to collect performance data through ping. However, WhatsUP Gold was able to provide greater information on Rascal, such as packet sent/lost, poll time, unavailable and percent available. DopplerVue is able to collect data, but the output only displays average packet loss.
- *Performance Data Analysis*: Both NM tools fail to provide any data analysis on Rascal.
- *Problem Reporting*: WhatsUp Gold was able to generate a report showing Rascal's connection state in a stop light method as seen in Figure 26. DopplerVue is able to generate a report designed to provide the top 5 through 25 alarms, however, it failed to collect alarm reports on Rascal, despite numerous occasions when Rascal's connections were turned off.



State Change Timeline

2001:480:211:1100::15 - Wednesday, May 14, 2008 12:00:00 AM - Thursday, May 15, 2008 12:00:00 AM

Start time	Monitor	State color	State	Duration	Message
Wednesday, May 14, 2008 11:02:33 AM	Ping		Down at least 20 min	25m	Request timed out
Wednesday, May 14, 2008 10:47:26 AM	Ping		Down at least 5 min	15m	Request timed out
Wednesday, May 14, 2008 10:44:24 AM	Ping		Down at least 2 min	3m	Request timed out
Wednesday, May 14, 2008 10:43:23 AM	Ping		Down	1m	Request timed out
Wednesday, May 14, 2008 10:34:18 AM	Ping		Up at least 5 min	9m	
Wednesday, May 14, 2008 10:30:17 AM	Ping		Up	4m	
Wednesday, May 14, 2008 10:29:16 AM	Ping		Down	1m	Request timed out
Wednesday, May 14, 2008 10:24:14 AM	Ping		Up at least 5 min	5m	
Wednesday, May 14, 2008 10:20:12 AM	HTTP		Up at least 5 min	23m	
Wednesday, May 14, 2008 10:20:11 AM	Ping		Up	4m	

Figure 26. DopplerVue (top) and WhatsUp Gold (bottom) alarm report, TNT08-03

- *Performance Data and Statistic Collection*: Both NM tools were able to provide some statistical data on Rascal; however, WhatsUp Gold was able to provide better, more in depth, analysis report on its data by providing poll time, unavailable time and percent availability.

More work in this area is required with much more in depth analysis than this thesis is able to provide. There is a great deal lacking in the outlined experimentation resulting from resource limitations and supporting documentation.

B. CONCLUSIONS

As DOD proceeds to mandate the implementation of IPv6 throughout the services, one key factor is overlooked. Research in tactical or edge network management, with an intent to identify potential management tools, in support

of IPv6 node management within the GIG is minimal at best. This thesis incorporated the theory behind the FCAPS model, concentrating specifically on Performance Management, to establish a set of metrics to measure existing IPv6 network management tools. Performance management metrics established in Chapter three serve to evaluate commercial network management tools currently used by DOD. These network management tools have preset parameters such as, network throughput, delays, bandwidth utilization; and attempt to monitor IPv6 sensors as they join the network. The CENETIX and NPS TNT field experimentation programs offer the opportunity to explore the concept of IPv6 network performance management by evaluating selected technologies to identify and address problems associated with the deployment of these tools in an operational tactical environment.

Network performance analysis of an IPv6 sensor on-the-move was conducted by using DopplerVue, What's Up Gold, and SolarWinds installed on separate computers running Windows XP Pro SP2 and Windows Vista. WireShark was implemented to monitor packet traffic and was installed on a laptop running Windows XP Pro SP2. An IPv4 topology was created to record the state of the OFDM testbed operation over a period of time and its ability to acquire active nodes. This provided a general picture of the edge network. IPv6 sensor nodes were then added into the OFDM network, and their performance was monitored by NM tools. This study helped identify desirable OS and NM tool combinations, shortfalls associated with each NM tool's inability to

detect and monitor IPv6 nodes, and different means to aggregate and present the most feasible metrics for each NM tool.

Analysis of TNT 08-02 and 03 experimentation results indicate, current NM tools are not able to actively detect and monitor IPv6 sensors on-the-move. Further study and experimentation can provide a clearer picture of the tools full potential and capabilities, which will lead to an optimal solution. Ultimately, the true solution to this problem will not become obvious until all functional areas of the FCAPS model are considered, measured, and tested for each of the tools under consideration. Greater attention is required not only in the DoD but throughout the commercial sector before an IPv6 sensors on the move can be properly monitored and managed.

C. FUTURE CONSIDERATIONS

Network management tools work well in IPv4 environments but tend to lose functionality when monitoring IPv6 nodes. Nonetheless, the same tools tend to provide as good a service when running on IPv6 capable operating systems, such as Vista. The difference between Windows XP Pro and Vista are significant and known to create problems with application compatibility. However, given the differences noted during the experimentation it is only reasonable to assume the differences experienced are due to Vista’s native IPv6 capability. If this is true then it is also reasonable to assume that IPv6 ready Operating systems are needed to monitor IPv6 nodes. To further examine the difference between our chosen network management applications the following experiment is proposed.

Two Dell desktop computers will continue to run Windows Vista and XP Pro as separate platforms. Each platform will have DopplerVue, What's Up Gold, and Solar Winds configured to perform the same tasks; each will also be configured to operate as an IPERF server. Two separate laptops will be introduced, one as an IPERF client thereby generating IPv6 HTTP and SNMP packets while the second laptop collects packet flow using Wireshark, as depicted in Figure 27. The IPERF packet generator should run for a minimum of four hours to allow sufficient generation of traffic to help validate findings.

All variables will remain constant as the intent is to measure how well a given monitoring tool is able to complete a desired task. Specifically, how well each tool is able to carry out each of the seven metrics as outlined in chapter three. Testing should be limited to four hours to facilitate scheduling considering time zone differences and primary duties. Additionally, packet data collected over four hours is a large amount of data to analyze, but much more manageable than if the test is run for longer periods of time. Also, shorter times help eliminate or manage anomalies created by interruptions caused by network service interruptions. Four hours will allow for replication of results to help validate findings and aid in the building of knowledge.

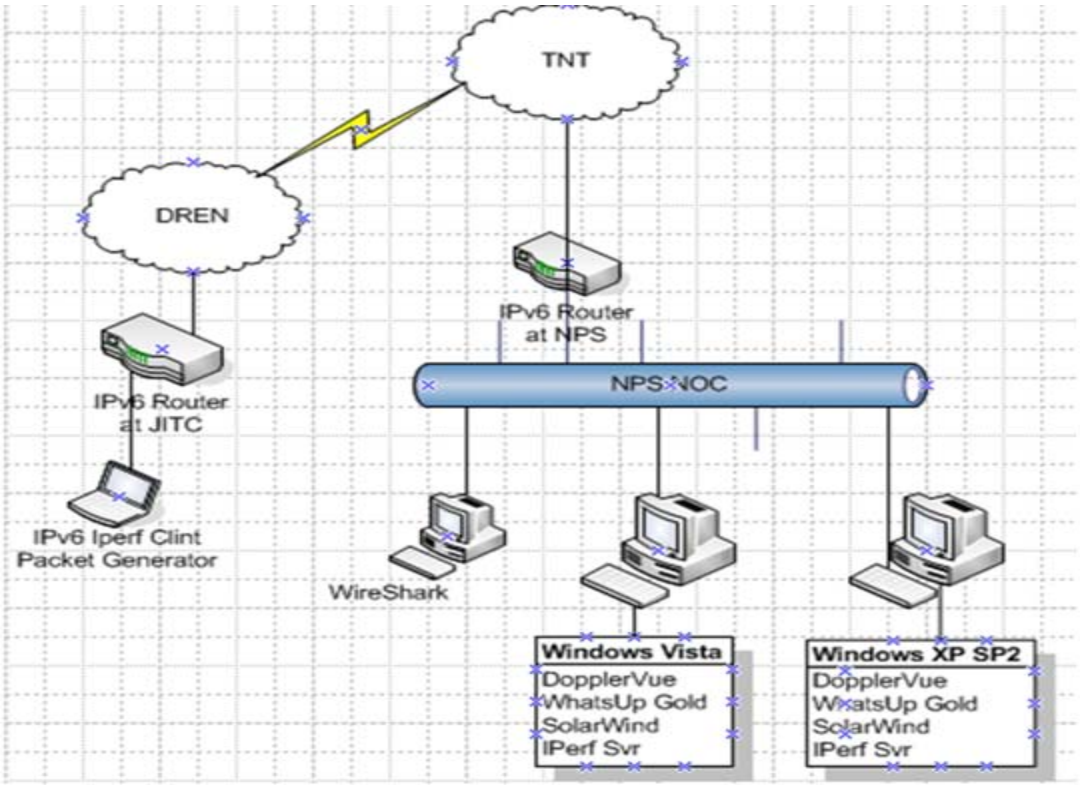


Figure 27. Proposed IPv6 experiment with JITC

The proposed experiment will help generate a greater understanding of how tactical IPv6 nodes can best be monitored. Additionally, this will allow for further study of FCAPS functional areas and help identify the ideal Network Operations Center environment required to monitor tactical IPv6 nodes. Furthermore, once the proper and preferred hardware and software suites are identified this study can be expanded to include a simulated tactical environment in which SOCOM personnel and equipment are included in the TNT architecture. Future work lends itself very well to an experimentation campaign. There are many aspects of IPv6 network management requiring further research. More can be gained by studying all functional areas of FCAPS over an extended period than we were able to

gain from our narrowly focused thesis. “The objective of a campaign design is to give comprehensive attention to all of the important influences on system performance” (Stenbit, 2002).

LIST OF REFERENCES

Alberts, D.S., Garstka, J.J., & Stein, F.P. (2000, February). *Network Centric Warfare: Developing and Leveraging Information Superiority,* 191-192. DoD C4ISR Cooperative Research Program.

Alberts, D.S., Hayes, R. (2003, October). *Code of Best Practice Experimentation.* DoD Command and Control Research Program.

Baumgartner T.J., & Phillips M.D. (2003, June). *Implementation of A Network Address Translation Mechanism Over IPv6*, Master's Thesis. Naval Postgraduate School, Monterey, California.

Boutaba, R., & Polyrakis, A. (2002, January). *Projecting Advanced Enterprise Network and Service Management to Active Networks Projecting FCAPS to Active Networks*. IEEE Network, 16, 28-33. Retrieved on February 2008 from http://ieeexplore.ieee.org/iel5/65/21121/00980542.pdf?tp=&isnumber=&arnumber=980542.

Donnelly, D. Email SUBJ: Ipswitch WhatsUp Gold Premium v12 Evaluation. Emails dated May 16, 2008.

CIO Council Architecture and Infrastructure Committee (AIC) (2006, February). *IPv6 Transition Guidance.* Retrieved on January 2008 from www.cio.gov/documents/IPv6_Transition_Guidance.doc.

CISCO (2006, April). *IPv6 Advance Concept.* RST-3300.

Internet Protocol Handbook. (No Date Given) Cisco. Retrieved on June 2008 from http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Internet-Protocols.html.

CISCO System. 2800 Model Comparison. Retrieved on April 2008 from http://www.cisco.com/en/US/products/ps5854/prod_models_comparison.html.

Comer, D.E. (2000). *Internetworking with TCP/IP Principle, Protocols, and Architectures*. New Jersey: Prentice Hall.

DACS (No Date Given). A History of Software Measurement at Rome Laboratory. Retrieved on April 2008 from http://www.dacs.dtic.mil/techs/history/His.RL.2.2.html

Davis, J.A. (2005, March). *An Analysis of Network and Sensor Performance Within IEEE 802.X Wireless Mesh Networks in The Tactical Network Topology*, Master's Thesis. Naval Postgraduate School, Monterey, California.

Dean, T. (2005, July). *Network plus Guide to Networks, Fourth Edition.* Thomson Course Technology.

Defense Information Systems Agency (DISA) (2006, September). The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan.

Department of Defense Chief Information Council (CIO) Memorandum (2005, August 16). SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6). Retrieved on March 2008 from http://www.disa.mil/gs/dsn/webfiles/IPv6_DoD_Response_to_OMB_Guidance_16_Aug_2005.pdf.

Doan, T. (2006, June). Science Applications International Corporation (SAIC). White paper. *IPv6 Security Assessment*.

Federal Enterprise Architecture (FEA) (2008, January) *Results of FY 2007 Federal Enterprise Architecture Assessment.* Retrieved May 2008 from http://www.whitehouse.gov/omb/egov/documents/2007_EA_Assessment_Results_Summary.pdf.

Forouzan, B.A. (2003, July). *TCP/IP Protocol Suite, Second Edition.* New York: McGraw-Hill.

Gateau,J. (2007, March) *Extending Simple Network Management Protocol (SNMP) beyond network management: a MIB architecture for network-centric services*, Master's Thesis. Naval Postgraduate School, Monterey, California.

Government Accounting Office (GAO) (2005, May). *Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks*. Retrieved on April 2008 from http://www.gao.gov/new.items/d05471.pdf.

Goldszmidt G., & Yemini Y. (1998, March). *Delegated Agent for Network Management.* IEEE Communications Magazine.

Hagen, S. (2006, May). *IPv6 Essentials, Second Edition*. California: O'Reilly.

Haines T.J., & McFerron M.P. (2006, September). *LRV: Enhancing Command, Control, Communications, and Computers and Information Systems (C4I) to Tactically Employed Forces via a mobile Platform.* Master's Thesis. Naval Postgraduate School, Monterey, California.

Heilbronner, S. (1997, October). *Managing PC Network.* IEEE Communication Magazine. Retrieved on April 2007 from http://ieeexplore.ieee.org/iel1/35/13573/00623994.pdf?tp=&isnumber=&arnumber=623994.

ICMP. ICMP Types and Codes (No Date Given). Retrieved on June 2008 form http://spirit.com/Resources/icmp.html.

IPv6 (2006, January). IPv6 Task Force, U.S. Department of Commerce, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv*6). Retrieved on February 2008 from http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6finalTOC.htm.

Johnson D., Perkins C., & Arkko J. (2004, June). *Mobility Support in IPv6,* RFC 3775.

Jilong, W., Chunsheng, N., Jianing, W. (2004). Next Generation Internet. IEEE Computer Society. Retrieved on March 2008 from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1300504

Kaushik, D. (No Date Given). *IPv6 and the Military.* Retrieved on 01 April 2008 from http://www.ipv6.com/articles/military/Military-and-IPv6.htm.

Loshin, P. (2004). *IPv6: Theory, Protocol, and Practice*. California: Morgan Kaufmann.

Makela, J. (1999, April). *Management of Public IP Networks.* Whitepaper. Helsinki University of Technology.

Microsoft, Co. (2008, January). *Introduction to IP Version 6. W*hite Paper.

Help & Support. Microsoft, Co. (No Date Given). Internet Control Message Protocol Basic. Retrieved on June 2008 from http://support.microsoft.com /kb/170292.

Morton, D. (1997, May). *Understanding IPv6*. Issue 83. PC Network Advisor.

Office of ASD (NII)/DoD CIO (2004, December). *Data Sharing in a Net-Centric Department of Defense*, Unclassified\\For Official Use Only. Department of Defense (DoD).

Office of ASD (NII)/DoD CIO (2006 September). *The Department of Defense (DoD) internet protocol version 6 (IPv6) Transition Plan*, Version 2, Unclassified\\For Official Use Only. Department of Defense (DoD).

OMB (2005, August 2). Office of Management and Budget (OMB)memorandum 05-22. SUBJECT: *Transition Planning for Internet Protocol version 6 (IPv6)*. Retrieved on March 2008 from http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf.

OMB (2007, October 25). Office Of Management and Budget (OMB)memorandum, Subject: *Instruction for Agency Self-Assessment and Submission of Enterprise Architectures for Annual OMB Assessment.* Retrieved on April 2008 from http://www.whitehouse.gov/omb/egov/documents/EA_Assessment_Ver22_and_Submission_Instructions_Memo_20071025.pdf.

O'Neal, M.R. (2003, June). A Design Comparison Between IPv4 and IPv6 in The Context of MYSEA, and Implementation of an IPv6 MYSEA Prototype, Master's Thesis. Naval Postgraduate School, Monterey, California.

Parker, J. (2005, May). *FCAPS, TMN & ITIL: Three Key Ingredients to Effective IT Management*. White Paper. Retrieved on March 2008 from http://www.openwatersolutions.com/docs/FCAPS_TMN_%20ITIL.pdf.

CISCO et al (2001, September). *Internetworking Technologies Handbook*. Indiana: Cisco Press.

Perkins, C. (2002, August). *IP Mobility Support for IPv4,* RFC 3344.

Raman, L. (1998, March). *OSI Systems and Network Management*. IEEE Communication Magazine, 3(38). Retrieved on March 2008 from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=663327.

Rusu O., & Manolache F.B. (No Date Given). *Network Management Framework: A Distributed Virtual NOC Architecture.* Mellon College of Sciences. Retrieved on February 2008 from http://conference.iasi.roedu.net/site/conference/papers/RUSU_O-Network_Management_Framework.pdf.

Stallings, W. (1998, March). SNMP and SNMPv2: The Infrastructure for Network Management. IEEE Communications Magazine. Retrieved on June 2008 from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=663326.

Stewart, D.F., Turner, E.G. (2006, March) *Solution Analysis of Universal Wireless Joint Point Technologies for Heterogeneous Tactical Networks*, Master's Thesis. Naval Postgraduate School, Monterey, California.

Stevenson, D.W. (1995, April). *Network Management: What it is and what it isn't.* Tutorial. Retrieved on February 2008 from http://www.sce.carleton.ca/netmanage/NetMngmnt/NetMngmnt.html.

Thomson S., & Narten T. (1998, December). *IPv6 Stateless Address Autoconfiguration*, RFC 2642.

United States Special Operations Command (USSOCOM). (No Date Given). *Internet Protocol Version 6 (IPv6).* White paper.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Naval Postgraduate School
   Monterey, California

4. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

5. Michael Clement
   Naval Postgraduate School
   Monterey, California